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
旅かえる
Hit-Point Co.,Ltd.
漢化中文版攻略for
cherisher
免費
漢化中文版助手 for
厦门漫的信息技术有限
免費
旅行青蛙（旅かえる
arteoning
免費
青蛙旅行(中文漢化
VEGA STUDIO
免費
攻略 for 旅行青蛙
momdream
Guide for Tabikaeru
Mey Media
貓咪公寓 - Cat Con
Zepni Ltd.
Tabikaeru (旅かえる
To Be Honest
青蛙旅行-欢乐跳
Hangzhou Yanguo Tech

不同平台流竄修改APK、破解APK

編譯 VS 反編譯

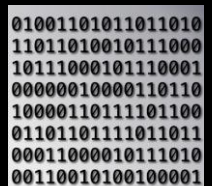
C#

Compile

IL(Intermediate Language)

Assemble

CLR(Common Language Runtime)/JIT

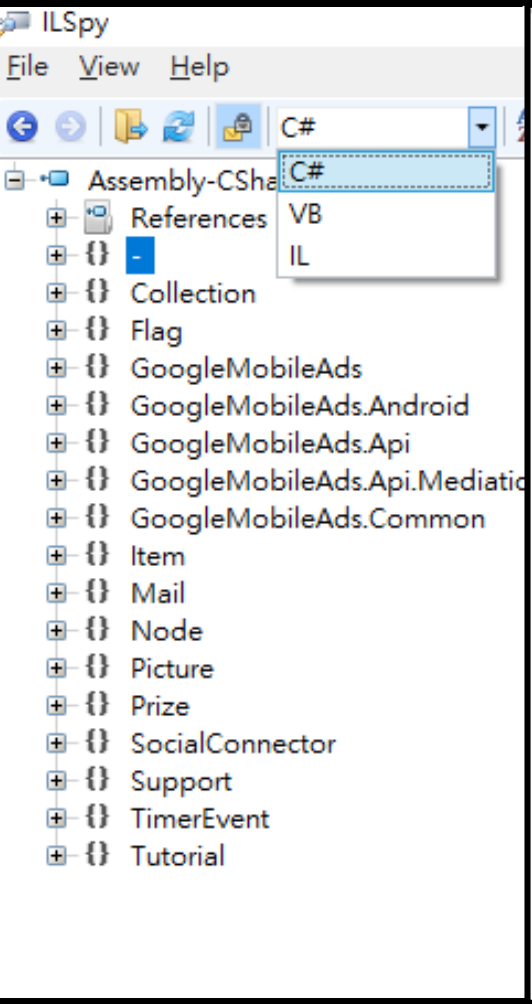


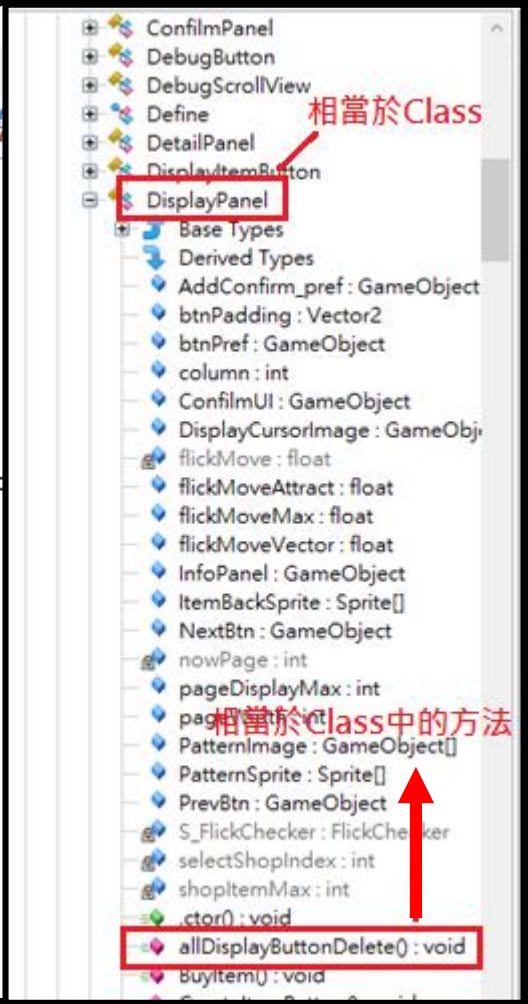
ILSpy

decompile

Unity3D遊戲(旅行青蛙)
Assembly-CSharp.dll

C#程式碼



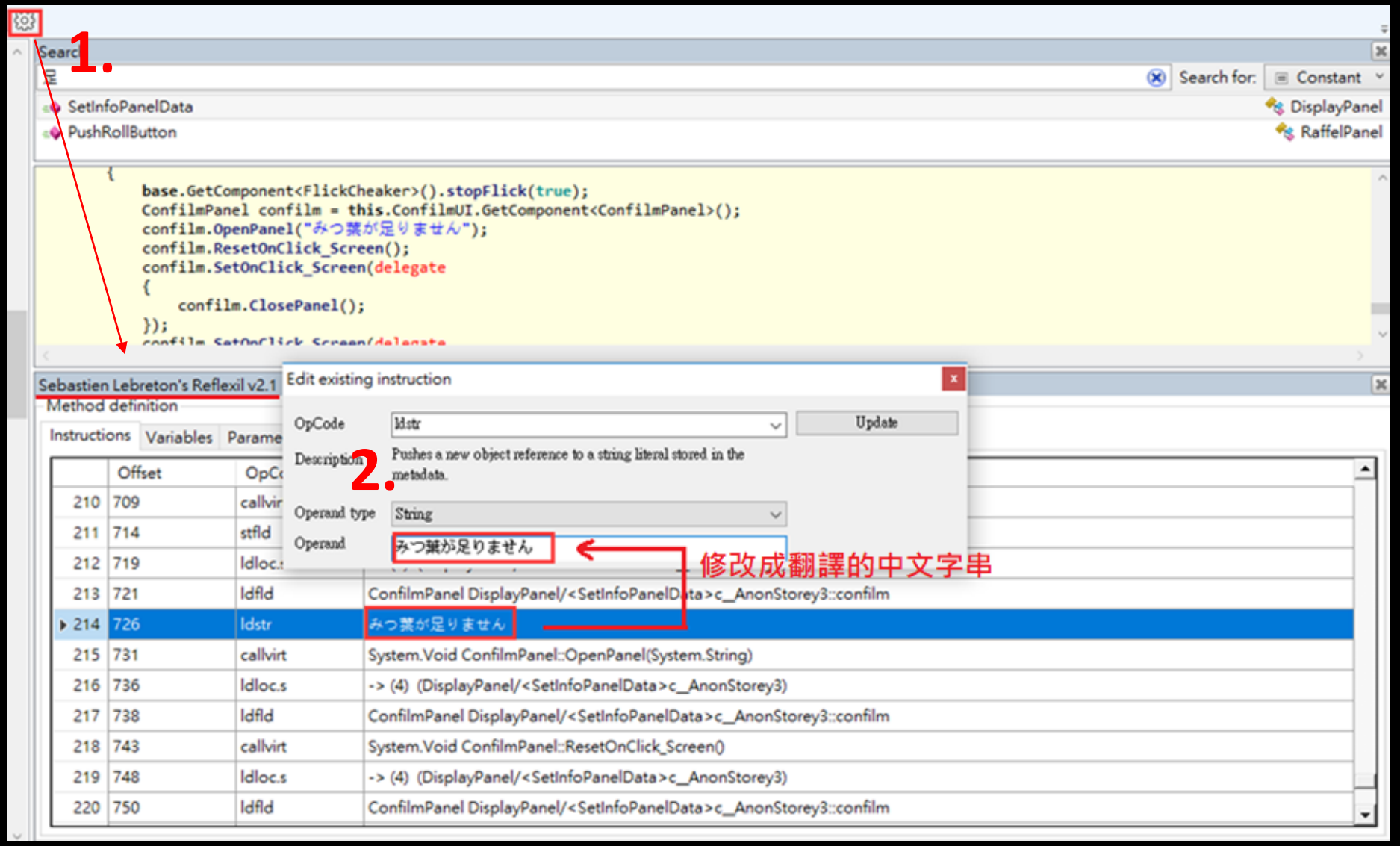



```
// DisplayPanel
public void allDisplayButtonDelete()
{
    IEnumerator enumerator = base.transform.GetEnu
    try
    {
        while (enumerator.MoveNext())
        {
            Transform transform = (Transform)enume
            if (transform.name.Equals("DisplayIter
            {
                UnityEngine.Object.Destroy(transfo
            }
        }
    }
    finally
    {
        IDisposable disposable;
        if ((disposable = (enumerator as IDisposab
        {
            disposable.Dispose();
        }
    }
}
```

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)



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);
        });
    }
}
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();
```

1.

2.

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

.cctor

```
// 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>
    {
```

白玉

1.

夜神模擬器 6.0.2.0

9:39

files

/sdcard/Android/data/jp.co.hit_point.tabikaeru

FILES APP

902.26MB used, 60.60GB free, r/o Mount R/W

..

Parent folder

Picture

19 2月 18 09:37:00 rwxrwx---

2.

Tabikaeru.sav

19 2月 18 09:37:00 2.09K rw-rw----

HEX Editor

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

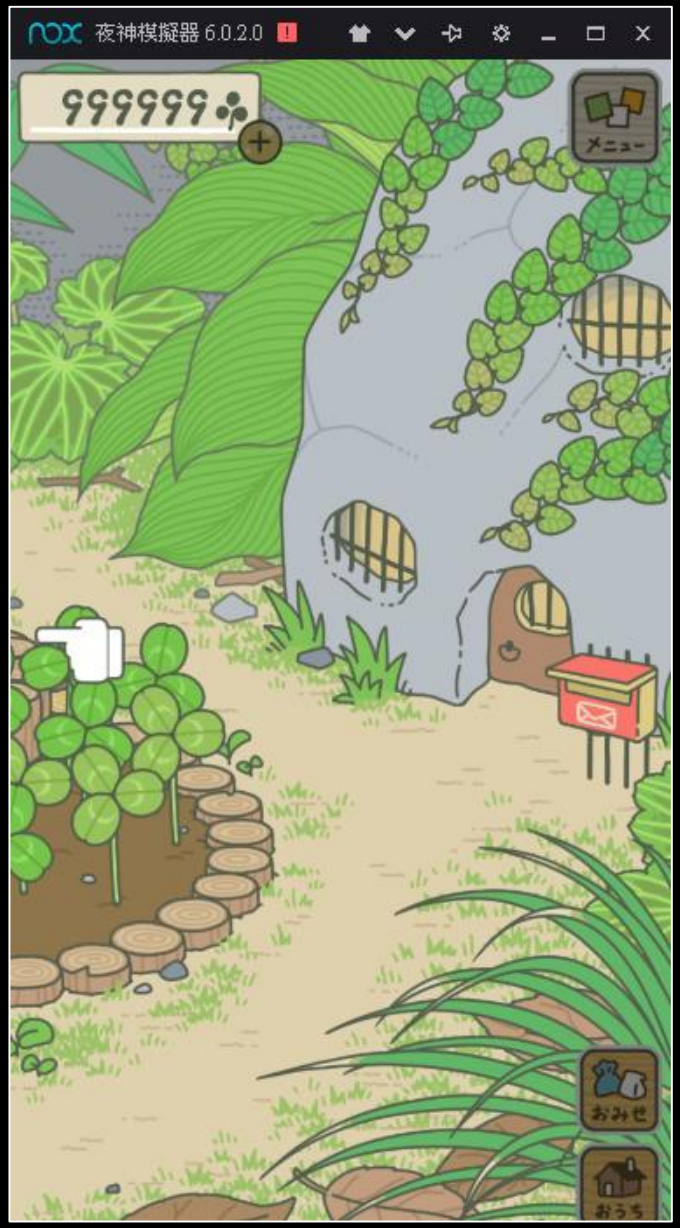
文件(F) 編輯(E) 搜尋(S) 檢視(V) 分析(A) 附加(X) 視窗(W) 關於(A)

16 | ANSI | 十六進位

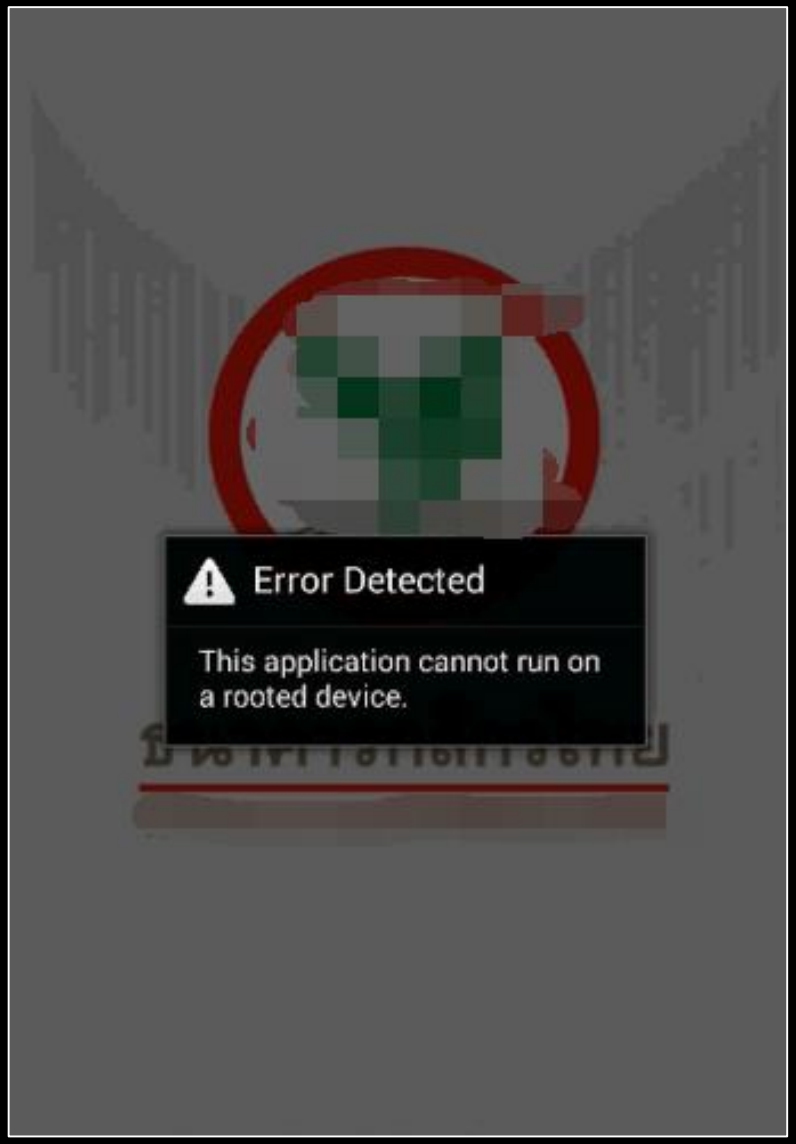
Tabikaeru.sav

三葉草數量

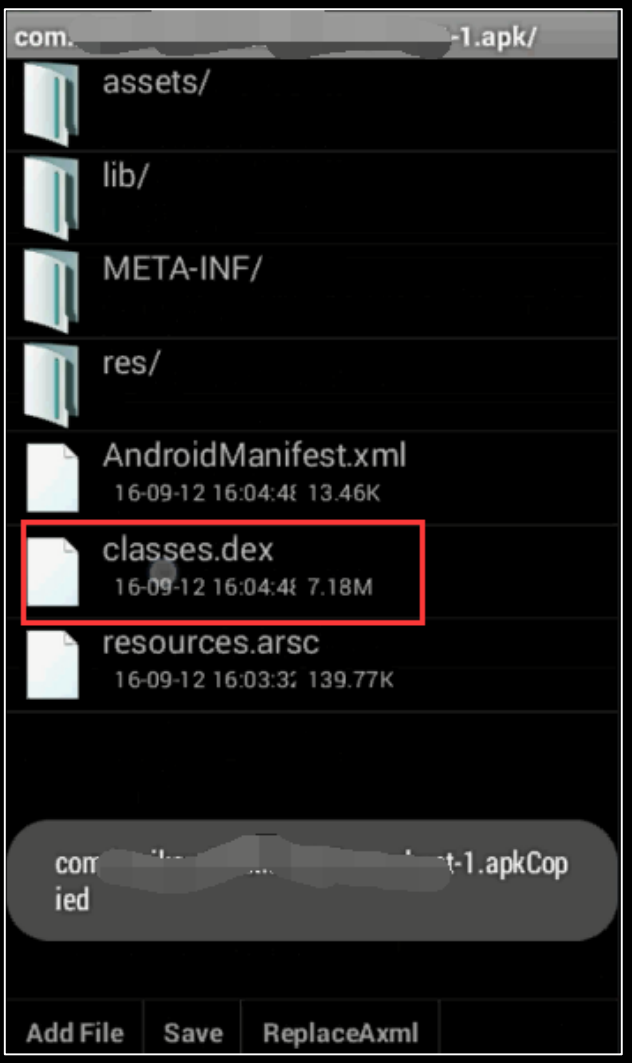
Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	00	00	29	04	00	00	00	00	00	00	00	0A	00	00	00	00
00000010	00	00	00	00	00	00	00	0F	42	3F	00	00				
00000020	00	14	FF	FF	A5	92	00	00	00	4E	00	00	00	01	00	00
00000030	00	00	00	00	00	01	00	00	00	07	00	00	07	B2	00	00
00000040	00	01	00	00	00	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

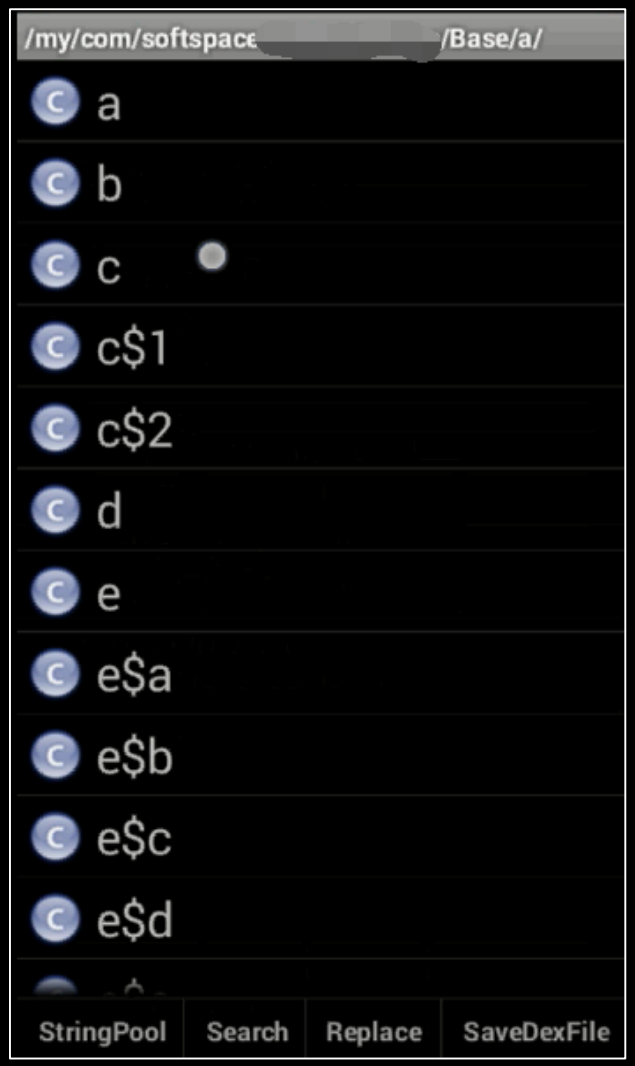


4.逆向分析(國外銀行被破解root偵測)

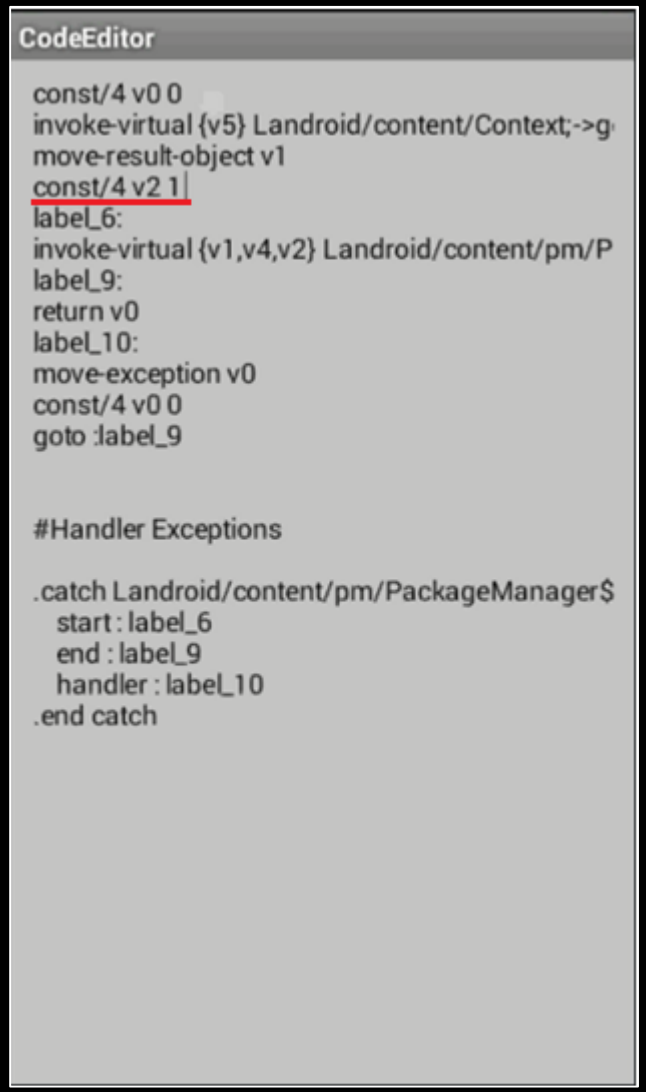


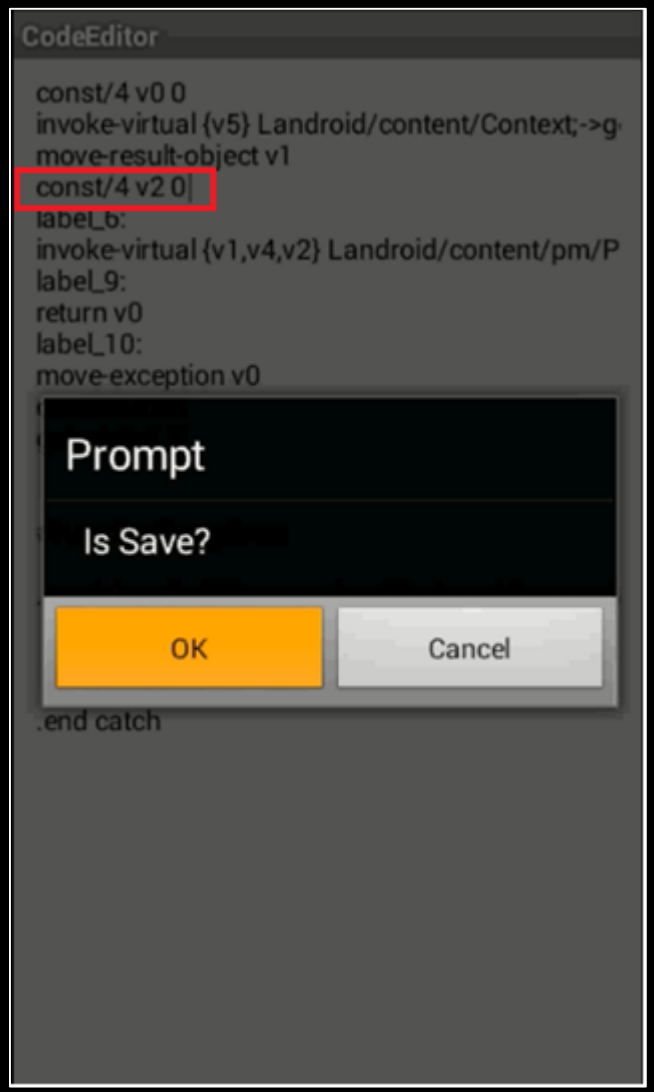
Dalvik Bytecode Editor





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

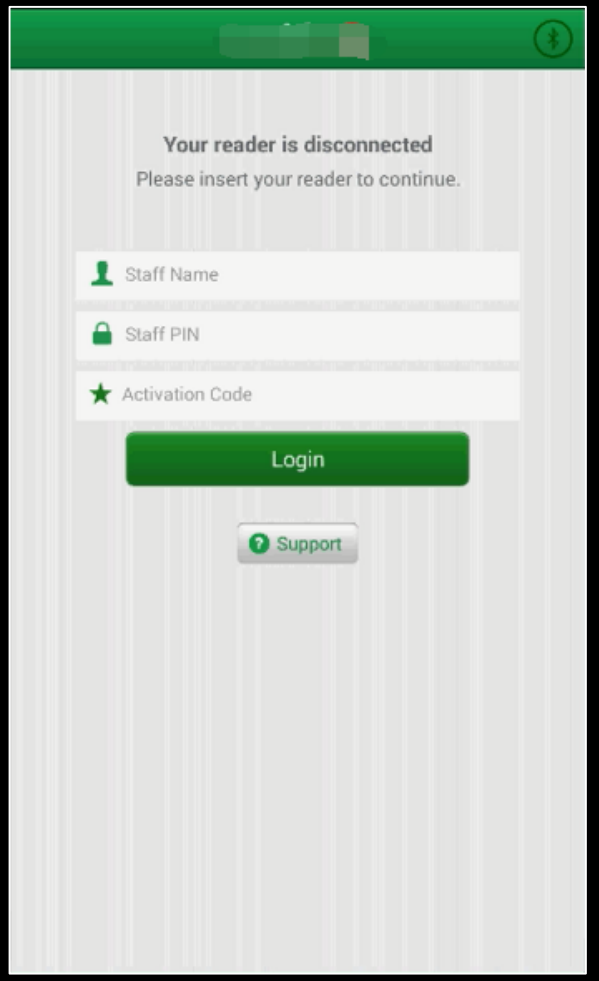




Root偵測失效


/sdcard/Download
Total Size:61.48G,Free Size:59.34G
..
???? 16-12-07 18:48:3
other
???? 16-11-02 17:56:5
com.
-1.apk
com.
t-1.signed.apk
二次打包的
修改APK


ธนาคารกสิกรไทย


Your reader is disconnected
Please insert your reader to continue.
Staff Name
Staff PIN
Activation Code
Login
Support

5.通用外掛(幸運破解器Lucky Patcher)

破解內購


幸運破解器
旅かえる
找到谷歌廣告！
找到應用內購！
Cydia Substrate
未發現！
Google Play 商店
有客製化破解可以使用！
找到應用內購！
破解結果
支援模擬破解應用程式內購和權限驗證庫:
破解模式 N1 - 成功...
破解模式 N2 - 成功...
破解模式 N3 - 失敗...
破解模式 N4 - 失敗...
********** 您有 28.0% Lu+的運氣！ 請啟動應用程式進行測試。 如果應用程式不能正確或正常運作，請重新安裝，並且不要再破解於該版本。
啟動
確定


909
メニュー
破解應用內購...
你想嘗試免費取得這個項目嗎？
發送 回復(reply) 命令給未簽名的應用程式（這可能適用於無 Root 的使用者）
儲存購買以便還原
使用當前設定自動重復購買
取消
確定
腳本及程序由 Dschuermann(Dominik) 編寫
若要停用自動重復購買您必須點選應用程式，然後轉到 "工具"->"移除已選擇並儲存的購買" 刪除已購買的項目。
- 為了達到最佳效果，您必須進行 Android 核心破解的\簽名驗證始終真實\；
- 要停用此破解請到底部的 \開關\ 面板裡選擇 \停用模擬 Google 購買\。


1309
メニュー
クローバーこうにゅう
× 400
0.91
みつ葉400
を購入しました
× 2800
0.88
特定商取引法に基づく表記

6.通用外掛(GameGuardian或燒餅修改器)

修改記憶體的資料


http://gameguardian.net/download
[2516] 旅かえる
76601DB8 479
編輯76601DB8 為 Dword
輸入 -2,147,483,648 到 4,294,967,295 之間的數值
數值: 99999
增加此值，不取代
凍結: 正常
另存為: Var #76601DB8
否
移至
是


99999
メニュー
おみせ
おうち

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

讚 156　Share　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。

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

是否可以反編譯

否

是否可以監測記憶體

否

放棄 Or 找其他

看到原始碼

竊取重要資料

動態監測

攻擊成功透過SMS感染

是否可以注入

否

放棄 Or 找其他

修改成功丟出修改包欺騙使用者造成傷害

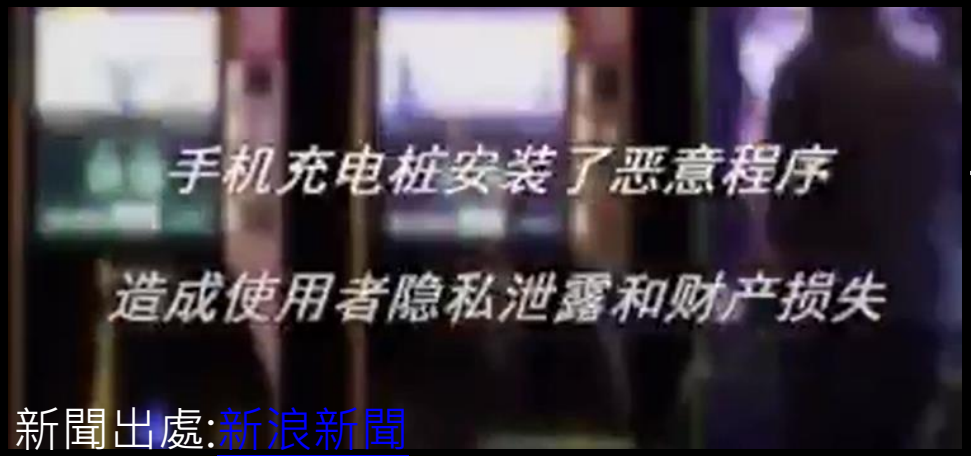
是否可以修改

否

放棄 Or 找其他

APP安全防護

使用者如何避免惡意程序感染



新聞出處:新浪新聞
影片連結: https://v.qq.com/x/page/s0385ej201n.html

避免使用免費插座

SMS簡訊網址不要亂點

聊天軟體網址不要亂點

● 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
遊戲交流
遊戲下載
手機影視
桌布主題
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]
查看: 1169 | 回覆: 5 | 好評: 0
Creppie | 收聽TA | 只看該作者 | 倒序瀏覽


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
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r
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
發表於 2016-11-9 00:35


腾讯视频
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
0:02:10
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

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

對應資安措施

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)

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

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

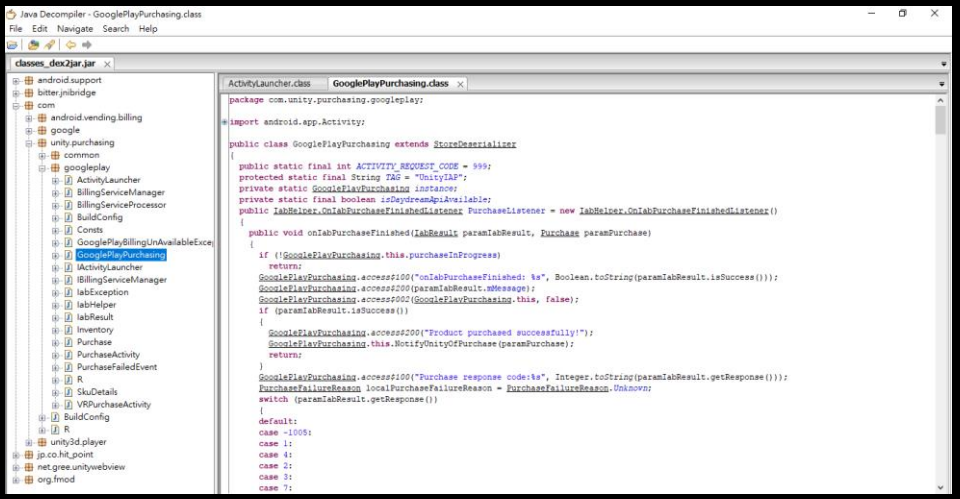
敏感資料 加密及綁定

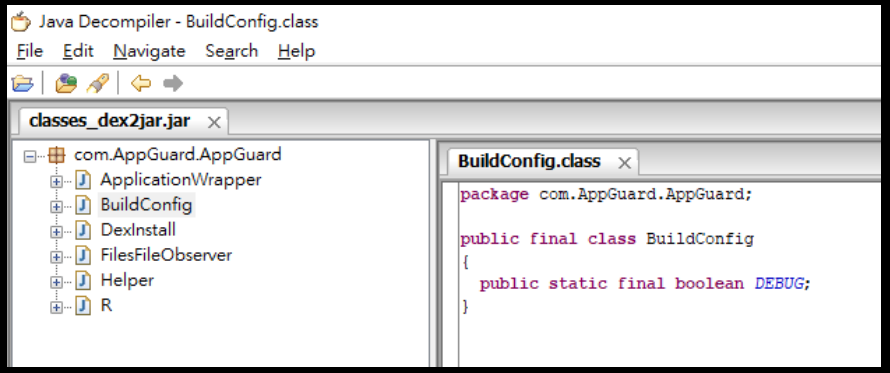
- 針對APP敏感性資料 做完整加密
- 加密技術使用AES對稱性加密演算法 金鑰長度256 bits 金鑰使用白箱加密保護
- 客製化檔案加密

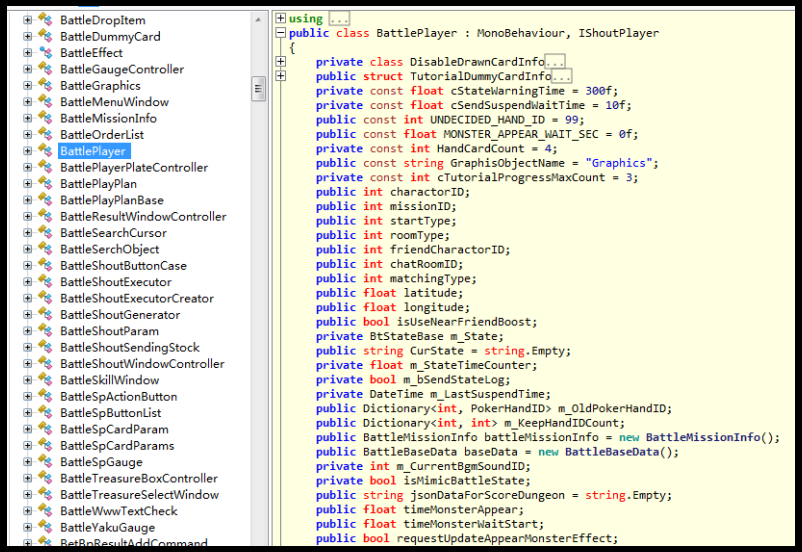
●防止逆向工程阻止反編譯

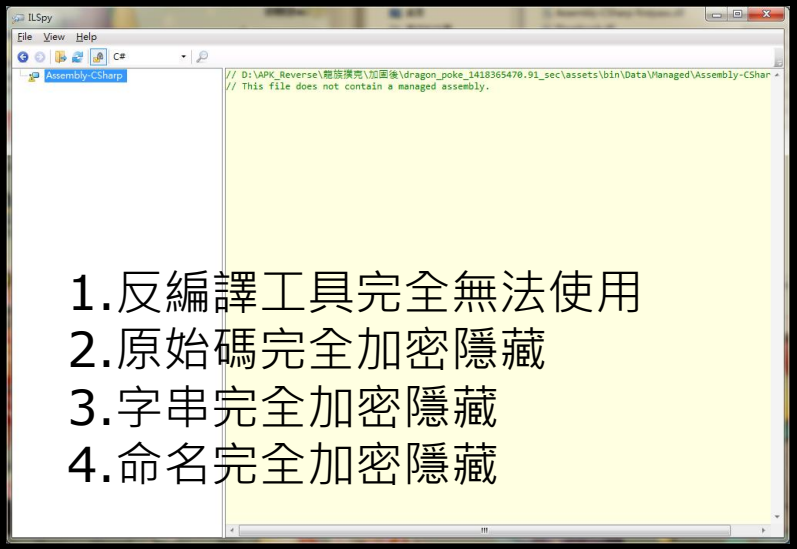
保護前

保護後



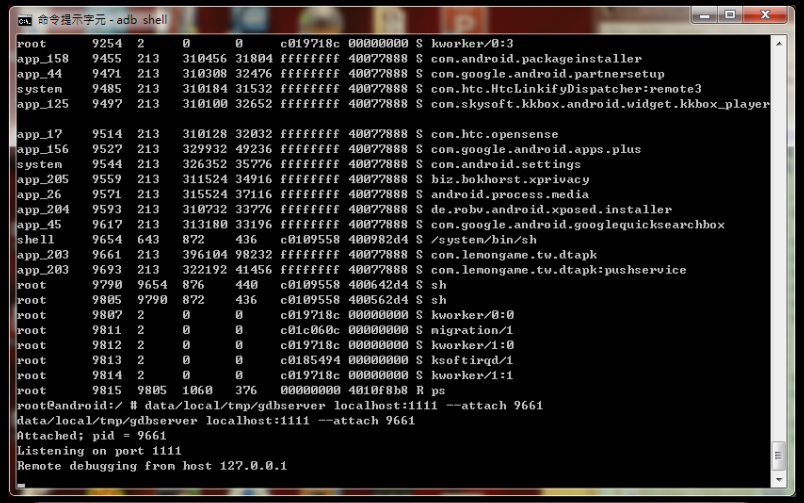


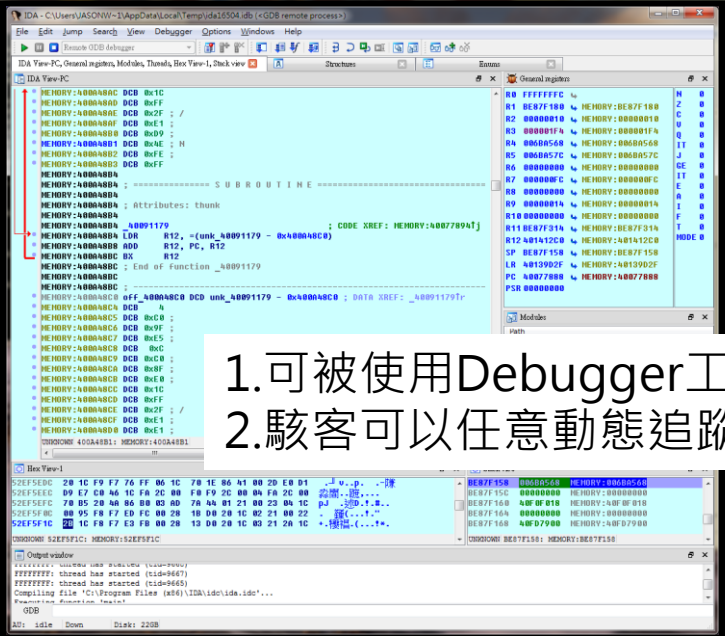




●阻擋Debugger防記憶體被修改

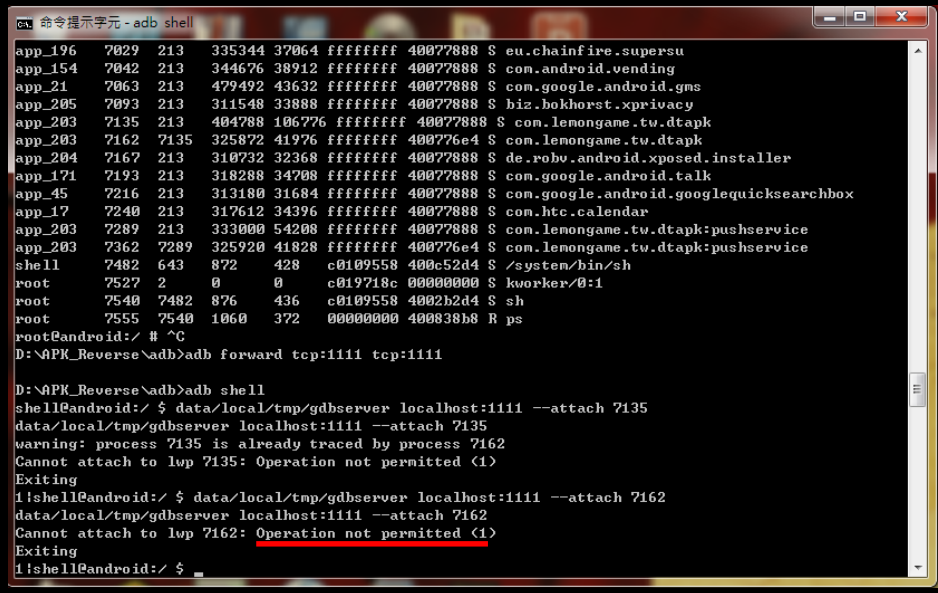
保護前





1.可被使用Debugger工具
2.駭客可以任意動態追蹤

保護後



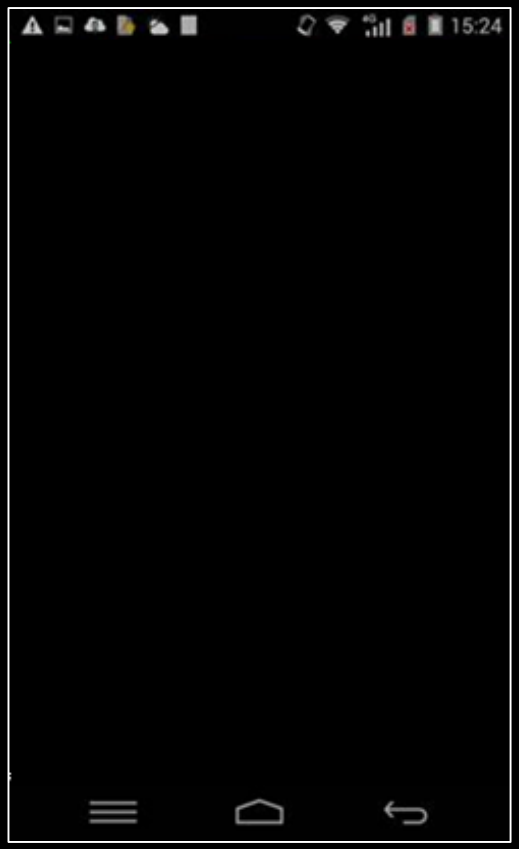
1.無法使用Debugger工具
2.讓駭客無法任意動態追蹤
3.讓記憶體相關的攻擊確定失效

●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



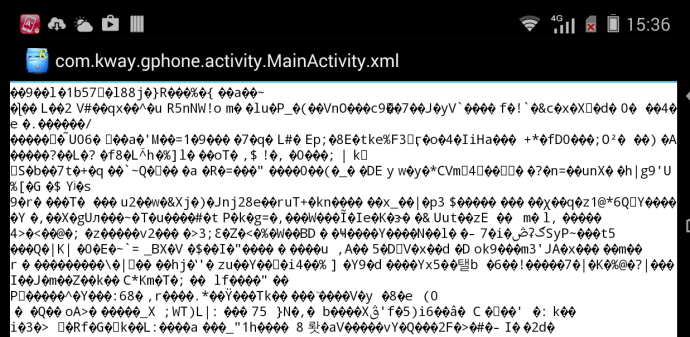
1.只要被竄改就Crash
2.避免市面上出現修改包

●敏感資料加密及綁定

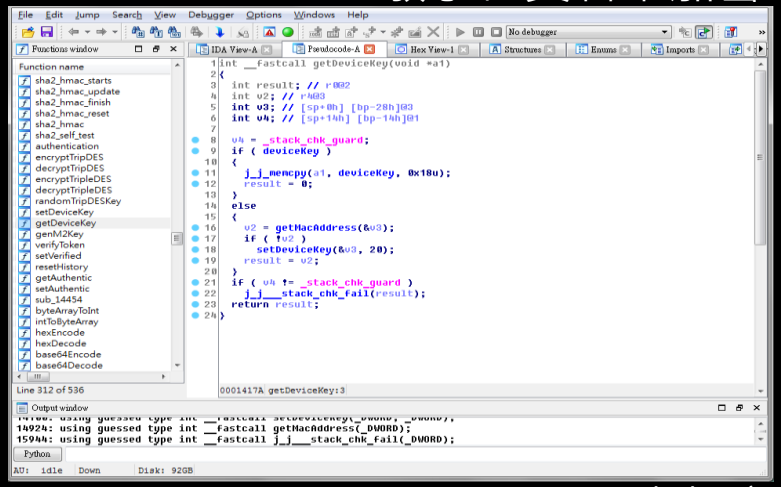
保護前

保護後

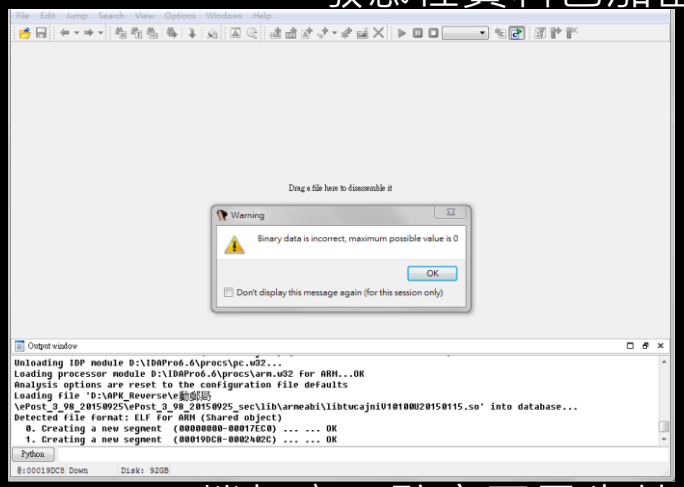
敏感性資料未加密



敏感性資料已加密



SO檔未加密

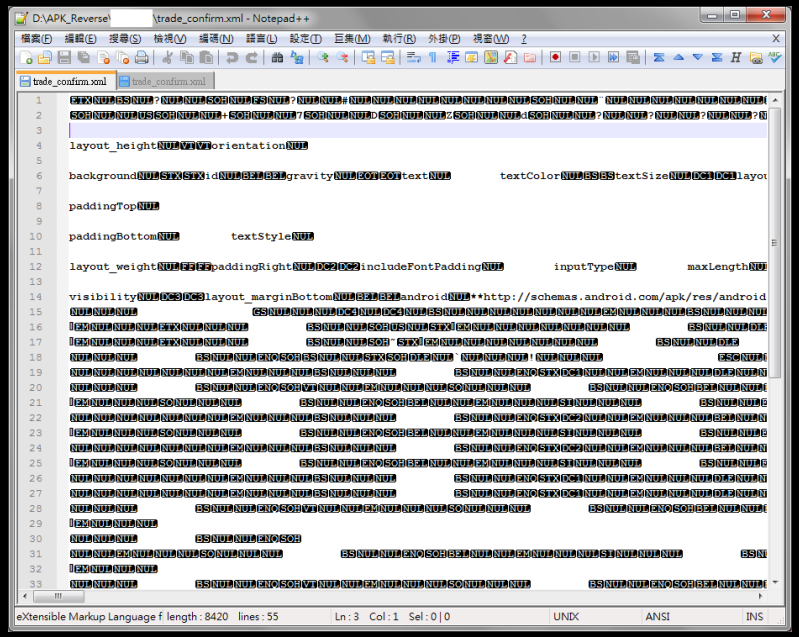


SO檔加密，駭客工具失效

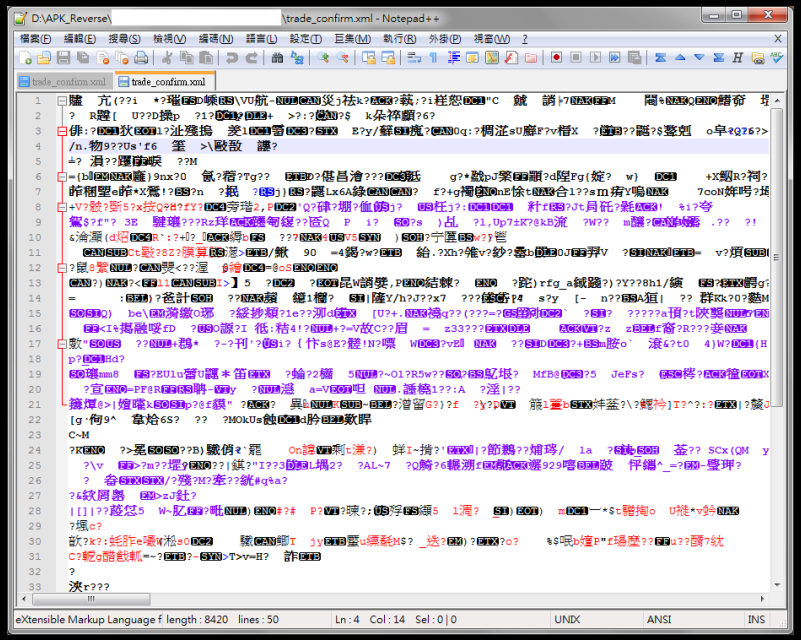
●敏感資料加密及綁定

保護前

保護後



APK內含資源檔未加密



APK內含資源檔已加密

是否可以反編譯

否

是否可以監測記憶體

否

放棄 Or 找其他

敏感資料加密及綁定

阻擋Debugger防記憶體被修改

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

否

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

否

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。