Android App
竄改及防範措施

Jason Wang 王羿廷

艾斯冰殼股份有限公司

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

About Me

王羿廷 Jason Wang

- 艾斯冰殼 ICEshell 創辦人暨執行長
- 專長
  - App 逆向工程
  - App 安全防護技術研發
- 研究成果
  - 台灣第一個國產 Android 加殼產品作者
  - 程式碼保護專利 M553450 發明人
  - 曾任 iThome CYBERSEC 講師
  - 曾任 CSA Taiwan Summit 講師

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

Table of Contents

- APK 檔案結構分析
- DEX 檔反編譯
- SO 檔反編譯
- APK 修改及二次打包
- 防範措施

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

APK 檔案結構

classes*.dex：Java/Kotlin 原始碼編譯後產生的二進位執行檔

lib 目錄：C/C++ 原始碼編譯後產生的二進位執行檔，副檔名為 SO

assets 目錄：App 會用到的資產檔，如音樂、影像、設定檔、Hybrid App 的 HTML 及 JS 檔等

res 目錄：App 會用到的資源檔，包含圖片、多國語系文字、UI 介面佈局等

AndroidManifest.xml：App 資訊清單，包含套件名稱、四大元件及權限宣告等

META-INF 目錄：APK 簽章相關檔案

resources.arsc：編譯後的資源索引檔

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

DEX 檔反編譯

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

DEX (Dalvik Executable) 檔 的產生

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

DEX 檔反編譯與重新編譯

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

逆向分析小技巧

如何從茫茫原始碼海中找出關鍵程式碼

1. 尋找 App 入口點
2. 搜尋字串
3. 搜尋系統 API 呼叫

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

尋找 App 入口點

在 AndroidManifest.xml 裡檢查 <application> 與 <activity> 元素：

1. 檢查 <application> 是否存在「android:name」屬性，若存在表示此 App 有自訂的 Application 類別，App 入口點即為該類別的 attachBaseContext() 或 onCreate() 方法。

2. 尋找包含 category 為「android.intent.category.LAUNCHER」的 activity 類別，此類別即為 App 的主要 activity，對於無自訂 Application 類別的 App，入口點即為主要 activity 類別的 attachBaseContext() 或 onCreate() 方法。

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

逆向分析小技巧

尋找 App 入口點

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0" package="owasp.mstg.uncrackable1">
    <uses-sdk android:minSdkVersion="19" android:targetSdkVersion="28"/>
    <application android:theme="@style/AppTheme" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:allowBackup="true">
        <activity android:label="@string/app_name" android:name="sg.vantagepoint.uncrackable1.MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
    </application>
</manifest>
```

1. <application> 裡無 android:name 屬性，此 App 無自訂的 Application 類別，故 App 入口點不在此處
2. category 為「android.intent.category.LAUNCHER」的 <activity> 為主要 activity，查看其 android:name 屬性
3. 此 App 入口點即為「sg.vantagepoint.uncrackable1.MainActivity.onCreate()」

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

搜尋字串

可在反編譯工具裡搜尋 App 出現過的錯誤訊息字串，快速定位到關鍵點

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

搜尋系統 API 呼叫

常見的系統 API 呼叫：

- 浮動式訊息：
  - Toast.makeText.show()
- 對話方塊：
  - new AlertDialog.Builder().create().show()
- 按鈕點擊事件：
  - OnClickListener()
- 關閉 App：
  - System.exit()
  - KillProcess()

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

SO 檔反編譯

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

Android SO (Shared Object) 檔的產生

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

SO 檔反編譯

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

逆向分析小技巧

如何從茫茫原始碼海中找出關鍵程式碼

1. 查看函數名稱
2. 搜尋字串
3. 搜尋系統 API 呼叫
4. 使用模擬執行工具分析程式行為

ICE SHELL

逆向分析小技巧

查看函數名稱

- 如果函數沒有特別宣告為 static，編譯後的 SO 檔使用逆向工具可查看完整函數名稱
- 為了便於維護，開發者通常會以該函數之功能為函數命名
- 看函數名稱即可了解該函數功用為何

start	.text	0000000000000E10
nullsub_1	.text	0000000000000E1C
j_nullsub_1	.text	0000000000000E20
sub_E24	.text	0000000000000E24
rand(void)	.text	0000000000000E4C
main	**.text**	**0000000000000F78**
megaInit(void)	.text	0000000000000FA4
sub_10E0	.text	00000000000010E0
goodbye(void)	.text	0000000000003080
sub_31B0	.text	00000000000031B0
sub_323C	.text	000000000000323C
Java_sg_vantagepoint_uncrackable3_MainActivity_init	.text	0000000000003310
Java_sg_vantagepoint_uncrackable3_MainActivity_baz	.text	0000000000003398
Java_sg_vantagepoint_uncrackable3_CodeCheck_bar	.text	00000000000033A4

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

逆向分析小技巧

搜尋字串

- 可在反編譯工具裡搜尋 App 出現過的字串，快速定位到關鍵點
- 搜尋逆向工具名稱，可找出偵測逆向工具的程式碼

.rodata:00000000000034C8	00000010	C	/proc/self/maps
.rodata:00000000000034DA	00000006	C	frida
.rodata:00000000000034E0	00000007	C	xposed
.rodata:00000000000034E7	0000000D	C	UnCrackable3
.rodata:00000000000034F4	00000023	C	Tampering detected! Terminating...
.rodata:0000000000003517	0000002E	C	Error opening /proc/self/maps! Terminating...

```
__int64 sub_30D0()
{
  __int64 v0; // x23
  const char *v1; // x2
  __int64 v3; // [xsp+0h] [xbp-230h]

  v0 = fopen("/proc/self/maps", "r");
  if ( v0 )
  {
    do
    {
      while ( !fgets(&v3, 512LL, v0) )
      {
        fclose(v0);
        usleep(500LL);
        v0 = fopen("/proc/self/maps", "r");
        if ( !v0 )
          goto LABEL_7;
      }
    }
    while ( !strstr(&v3, "frida") && !strstr(&v3, "xposed") );
    v1 = "Tampering detected! Terminating...";
  }
  else
  {
LABEL_7:
    v1 = "Error opening /proc/self/maps! Terminating...";
  }
  __android_log_print(2LL, "UnCrackable3", v1);
  goodbye();
  return sub_31B0();
}
```

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

逆向分析小技巧

搜尋系統 API 呼叫

常見的系統 API 呼叫：

- 字串相關：strcmp()、strncmp()、strstr()、strlen()、strcpy()、strncpy()...
- 檔案相關：open()、fopen()、fgets()、fputs()、read()、write()、close()、fclose()...
- 結束處理程序：exit()、_exit()、kill()、tkill()、tgkill()...

Address	Or	Name
0000000000015060		pthread_create
0000000000015068		__cxa_finalize
0000000000015070		ptrace
0000000000015078		_exit
0000000000015080		raise
0000000000015088		fclose
0000000000015090		__stack_chk_fail
0000000000015098		fgets
00000000000150A0		fork
00000000000150A8		strncpy
00000000000150B0		__android_log_print
00000000000150B8		strstr
00000000000150C0		usleep
00000000000150C8		getppid
00000000000150D0		malloc
00000000000150D8		waitpid
00000000000150E0		fopen
00000000000150E8		pthread_exit

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

逆向分析小技巧

使用模擬執行工具分析程式行為

- 面對較難分析的 SO 檔，可使用模擬執行工具進行分析：
  - unidbg (https://github.com/zhkl0228/unidbg)
  - AndroidNativeEmu (https://github.com/AeonLucid/AndroidNativeEmu)
- 使用方式請參考 2022 台灣資安大會「Android NDK 程式 (.so檔) 逆向與防逆向」(https://cyber.ithome.com.tw/2022/session-page/817)

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

APK 修改

及二次打包

ICE SHELL

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

修改版 APK 製作流程

原始 APK → 拆解 → 分析、修改 → 重新打包、簽章 → 修改版 APK → 散播至網路

拆解	分析、修改	重新打包、簽章
unzip/7-zip baksmali apktool	JADX IDA Pro Ghidra hex editor	smali apktool zip/7-zip jarsigner/apksigner

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

修改範例

OWASP MAS Crackmes：Android UnCrackable Level 1

- 用於練習逆向工程的 App
- 由 OWASP Mobile Application Security 所提供
- 修改目標：輸入任何字元都能顯示驗證成功
- 下載網址：https://mas.owasp.org/crackmes

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

APP 行為分析

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

逆向分析

字串搜尋與原始碼分析

- 在 JADX 裡搜尋錯誤訊息文字 Nope...，找出驗證函數 verify()
- 仔細閱讀原始碼，發現 if(a.a(obj)) 為關鍵判斷點

```java
public void verify(View view) {
    String str;
    String obj = ((EditText) findViewById(R.id.edit_text)).getText().toString();
    AlertDialog create = new AlertDialog.Builder(this).create();
    if (a.a(obj)) {
        create.setTitle("Success!");
        str = "This is the correct secret.";
    } else {
        create.setTitle("Nope...");
        str = "That's not it. Try again.";
    }
    create.setMessage(str);
    create.setButton(-3, "OK", new DialogInterface.OnClickListener() { // from c
        @Override // android.content.DialogInterface.OnClickListener
        public void onClick(DialogInterface dialogInterface, int i) {
            dialogInterface.dismiss();
        }
    });
    create.show();
}
```

https://github.com/skylot/jadx

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

逆向分析

smali 分析

- 將原始碼轉為 smali，發現 if(a.a(obj))

  對應的 smali 為 if-eqz p1, :cond_2b

- 使 if-eqz p1, :cond_2b 不成立即可顯

  示驗證成功

```
131     invoke-static {p1}, Lsg/vantagepoint/uncrackable1/a;->a(Ljava/lang/String;)Z
132
133     move-result p1
134
135     if-eqz p1, :cond_2b
136
137     const-string p1, "Success!"
138
139     invoke-virtual {v0, p1}, Landroid/app/AlertDialog;->setTitle(Ljava/lang/CharSequence;)V
140
141     const-string p1, "This is the correct secret."
142
143     :goto_27
144     invoke-virtual {v0, p1}, Landroid/app/AlertDialog;->setMessage(Ljava/lang/CharSequence;)V
145
146     goto :goto_33
147
148     :cond_2b
149     const-string p1, "Nope..."
150
151     invoke-virtual {v0, p1}, Landroid/app/AlertDialog;->setTitle(Ljava/lang/CharSequence;)V
152
153     const-string p1, "That\'s not it. Try again."
154
155     goto :goto_27
156
157     :goto_33
158     const/4 p1, -0x3
```

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

作業環境及準備工具

- MacOS
- JRE (Java Runtime Environment) or JDK
  https://www.oracle.com/java/technologies/downloads/
- Android Studio
  https://developer.android.com/studio
- smali/baksmali
  https://bitbucket.org/JesusFreke/smali/downloads/
- Vim 或文字編輯器
- 檔案及目錄結構

```
UnCrackable-Level1
|____UnCrackable-Level1.apk
|____smali-2.5.2.jar
|____baksmali-2.5.2.jar
```

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

完整步驟

1. unzip UnCrackable-Level1.apk -d UnCrackable-Level1
2. rm -r UnCrackable-Level1/META-INF
3. java -jar baksmali-2.5.2.jar disassemble UnCrackable-Level1/classes.dex -o UnCrackable-Level1/classes
4. rm UnCrackable-Level1/classes.dex
5. 使用 Vim 或文字編輯器開啟 UnCrackable-Level1/classes/sg/vantagepoint/uncrackable1/MainActivity.smali
   在 **if-eqz p1, :cond_2b** 前加上 **#** ，使該行變成註解，修改後存檔
6. java -jar smali-2.5.2.jar assemble UnCrackable-Level1/classes -o UnCrackable-Level1/classes.dex
7. rm -r UnCrackable-Level1/classes
8. cd UnCrackable-Level1; zip -r ../UnCrackable-Level1-repacked.apk *; cd ..
9. jarsigner -verbose -sigalg SHA256withRSA -digestalg SHA-256 -keystore ~/.android/debug.keystore UnCrackable-Level1-repacked.apk androiddebugkey -storepass android -keypass android -signedjar UnCrackable-Level1-repacked-signed.apk

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

DEMO

https://drive.google.com/file/d/17Wp3livrNs_SGU6KkG88P8fgXS00KPVi/view?usp=sharing

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

懶人工具：APK Explorer & Editor

- 本身也是一個開放原始碼的 Android App
- 反編譯及修改 DEX 檔
- 二次打包及重新簽章
- 專案網址：https://github.com/apk-editor/APK-Explorer-Editor
- 其他非開放原始碼同類工具：NP管理器、MT管理器、ApkCrack

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

DEMO

https://drive.google.com/file/d/1WlzyJcGyVxK0_QlRtlsOlXTdlgha_eHf/view?usp=share_link

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

防範措施

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

如何避免修改及二次打包

1. 程式碼混淆
   - proGuard：https://developer.android.com/build/shrink-code
   - BlackObfuscator：https://github.com/CodingGay/BlackObfuscator
2. 使用 C/C++ 開發 NDK 程式並搭配防逆向措施
   - Android NDK 程式 (.so檔) 逆向與防逆向：https://cyber.ithome.com.tw/2022/session-page/817
3. 完整性檢查 API
   - Android API：PackageManager.requestChecksums()
   - Google Play API：Play Integrity API
4. 商用 App 安全防護產品
   - ICEshell：https://iceshell.co

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL

Thanks for Listening

Email : jason@iceshell.co

https://github.com/jasonwang1018/iThome/tree/main/2023

Copyright © 2023 ICEshell Co., Ltd. All Rights Reserved.

ICE SHELL