Android アプリの逆コンパイル

DashO（難読化ソフト）の必要性について

株式会社エージーテック

Contents

1.　本資料について

本資料は、逆コンパイルの方法を詳細に紹介し、簡単にオリジナルソースレベルまで戻すことができることを体感して頂くために作成しました。具体的には、簡易なアンドロイド向けアプリを無料で取得できるツールで逆コンパイルし、java ソースレベルまで戻します。その後、弊社が販売している PreEmptive 社の難読化ツール DashO を使用することで、解析困難な状態になることも併せて紹介します。

DashO に関しては、静的なプロテクション以外にも、実行時における攻撃に対する検出と防御処置も用意しています。後者に関しては本編で触れませんが、ご興味のある方は、お問合せください。

2.　ソースコードを難読化する目的とは

一部のプラットフォーム（Java、Android、iOS、.NET など）では、無償の逆コンパイラにより、時間と労力をかけずに、実行ファイルまたはライブラリからソースコードを簡単に復元することができます。ソフトウェアベンダ、金融サービス業者、製造業者など、ソースコードに独占的なビジネスルールや重要なプログラムロジックを組み込んでビジネスを行っている場合にはリバースエンジニアリングは知的財産の損失、システムの脆弱性への攻撃など企業利益に影響を及ぼす大きなリスクとなります。

3.　逆コンパイルまでの手順

早速、逆コンパイルまでの手順を説明します。

逆コンパイル用にサンプルアプリを作成しました。簡易的な商品登録用のアプリになります。

（オリジナルソースコード、逆コンパイル後のソース、難読化アプリの逆コンパイルも公開しています。）

① apk ファイルを zip ファイルにリネームして、展開します。

app-release-unsigned.zip	2017/10/02 14:49	ZIP ファイル	1,292 KB

展開後…dex ファイルを取得します。

res	2017/10/02 14:55	ファイル フォルダー	
AndroidManifest.xml	2017/10/02 14:49	XML ドキュメント	3 KB
classes.dex	2017/10/02 14:49	DEX ファイル	2,621 KB
resources.arsc	1980/01/01 9:00	ARSC ファイル	214 KB

② dex ファイルから jar ファイルを取得します。無料ツール「dex2jar」を使用します。

③ jar ファイルを zip ファイルにリネームして、展開します。

classes-dex2jar.zip	2017/10/02 15:01	ZIP ファイル	1,828 KB

Class ファイルを取得します。

```
yapplication>dir /b
BuildConfig.class
DBAdapter$DBHelper.class
DBAdapter.class
MainActivity$1.class
MainActivity$2.class
MainActivity.class
MyListItem.class
R$anim.class
R$attr.class
R$bool.class
R$color.class
R$dimen.class
R$drawable.class
R$id.class
R$integer.class
R$layout.class
R$mipmap.class
R$string.class
R$style.class
R$styleable.class
R.class
SelectSheetListView$1$1.class
SelectSheetListView$1$2.class
SelectSheetListView$1.class
SelectSheetListView$MyBaseAdapter$ViewHolder.class
SelectSheetListView$MyBaseAdapter.class
SelectSheetListView.class
SelectSheetProduct$1.class
SelectSheetProduct.class
SelectSheetTable.class
```

④ class から java ファイルを取得します。無料ツール「jad」を使用します。

```
C:¥decompiler¥jad.exe -d ./sources -s iava -r *.class
```

Java ファイルを取得します。

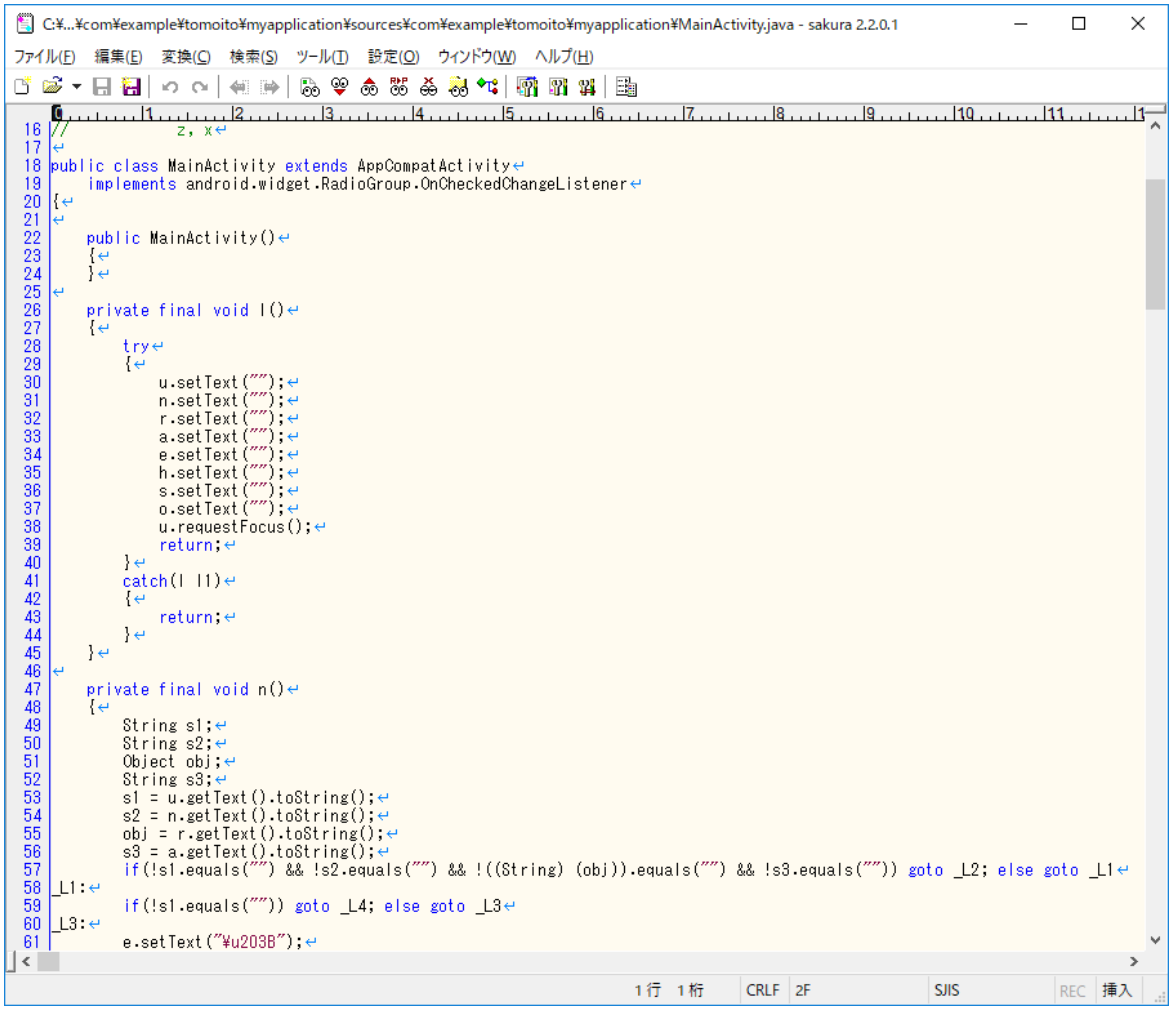
```
s¥com¥example¥tomoito¥myapplication>dir /b
BuildConfig.java
DBAdapter.java
MainActivity.java
MyListItem.java
R.java
SelectSheetListView.java
SelectSheetProduct.java
SelectSheetTable.java
```

⑤ java ファイルまで展開できれば、あとは中身を確認できます。
オリジナルのソースコードがなくてもどのようなロジックで DB に登録したり、登録した内容を ListView に表示したりすることが確認できます。今回サンプルで用意したソースには含まれていませんが、機密情報やセキュリティホールの脆弱等の特定にも有効です。お手元でご確認いただけるようオリジナルソースと逆コンパイル後のソースコードを公開しています。

⑥ 簡単に逆コンパイルができたところで、続いて DashO を通した後に、逆コンパイルを実施してみます。手順は上記の方法と全く同じです。見て頂いて分かりますが、java ファイル名も適当なアルファベットに置き換わっていることが分かります。

```
c.java
e.java
f.java
k.java
l.java
m.java
MainActivity.java
n.java
p.java
q.java
r.java
s.java
t.java
u.java
v.java
x.java
y.java
z.java
```

MainActivity.java 内の一部を紹介します。
解析が困難だということ一目でお分かりいただけます。仮に御社のアプリケーションがハッカーに狙われたとします。このようなソースコードを取得したハッカーは、対策が既に施されているアプリケーションと認識し、ハッキングを諦めざるを得ないという選択肢を取るのではないでしょうか。



4. まとめ

このように逆コンパイルの方法は容易です。さて、ここで二つの質問をします。

1) 御社のアプリケーションには、独自のアルゴリズムや収益を上げることのできる価値などの知的財産が含まれており、ハッキングが成功した場合に、収益が低下する可能性がありますでしょうか？
2) 御社のアプリケーションは、個人や組織のプライバシーや不正アクセスから保護されるべき機密情報を処理しますか？

もし上記二つの質問がいいえの場合は、難読化ツールを使用する必要性はございませんので、安心してください。しかし、上記の 1 つ以上が「はい」の場合、アプリケーションを「強化する」ことを強く検討する必要があるのではないでしょうか？

本資料で使用したツールの情報は以下になります。

1.「JAD」（JAVA デコンパイラ）について

作者：Pavel Kouznetsov

URL: http://www.kpdus.com （現在はアクセスできません）

入手先例 （JAD Java Decompiler Download ミラーサイト）

https://varaneckas.com/jad/

2.「dex2jar」（dex→class 変換ツール）について

作者：以下をご参照ください。

https://github.com/pxb1988/dex2jar/graphs/contributors

入手先例 （Git ハブ）

https://github.com/pxb1988/dex2jar

※製品に関するご質問がございましたら、お気軽に弊社営業部(sales@agtech.co.jp)までお問合わせください。