HACKTIVITY

Android Packers:

Separating from the pack

Ruchna Nigam

FortiGuard Labs,
FORTINET

11th October, 2014

FortiGuard Labs
Threat Research and Response

FORTINET

Today's Agenda

- What are Packers?
- Discussed in this talk
  - Pangxie
  - LIAPP
  - Bangcle
  - ApkProtect
- Packed Malware in the Wild
- Detection

Packers

What are Packers

- Mainly just compression eg: ZIP, RAR

Packers

What are Packers

- Mainly just compression eg: ZIP, RAR
- Runtime Packers or Executable Compression
  - Executable Russian Dolls
  - 'Outer' executable unpacks contents of 'inner' executable into memory and executes

Packers

What are Packers

- Mainly just compression eg: ZIP, RAR
- Runtime Packers or Executable Compression
  - Executable Russian Dolls
  - 'Outer' executable unpacks contents of 'inner' executable into memory and executes
- Widely used in Windows malware : UPX

Packers

Relevance in Android Security?

- Intended Use
  - Code hiding
  - Tamperproofing

Packers

Relevance in Android Security?

- Intended Use
  - Code hiding
  - Tamperproofing
- Flipside
  - Used on malware
  - Anti-hacker = Anti-analyst?

Pangxie

Pangxie

Static Analysis

- 'com.merry.wapper.WapperApplication'

```
<?xml version="1.0" encoding="utf-8"?>
<manifest android:versionCode="2" android:versionName="
1.1" package="com.joytap.PetDash"
  xmlns:android="http://schemas.android.com/apk/res/
  android">
    <application android:theme="@*android:style/Theme.
    Black.NoTitleBar.Fullscreen" android:label="@string/
    app_name" android:icon="@drawable/ic_launcher"
    android:name="com.merry.wapper.WapperApplication">
```

Pangxie

Static Analysis

- 'com.merry.wapper.WapperApplication'
- WapperApplication.class

```
public class WapperApplication extends Application
{
  static
  {
    System.loadLibrary("nsecure");
  }

  private native void validate(Context paramContext);
```

Static Analysis

- 'com.merry.wrapper.WrapperApplication'
- WapperApplication.class
  - Loads library 'nsecure.so'
  - Calls native function **validate**

```
public class WapperApplication extends Application
{
  static
  {
    System.loadLibrary("nsecure");
  }

  private native void validate(Context paramContext);
```

Static Analysis - libnsecure.so

- Exports

digestDecrypt	4B881D34
AESDecrypt	4B881B80
classDestroy	4B881B1C
classInit	4B881A68
strToJstring	4B8819FC
dexDecrypt	4B881924
Java_com_merry_wapper_WapperApplication_validate	4B8818C4
decryptDex	4B88183C
verifyDigest	4B8813B8

Static Analysis - libnsecure.so

- Exports
- Java_com_merry_wapper_WapperApplication_validate

```
        EXPORT Java_com_merry_wapper_WapperApplication_validate
Java_com_merry_wapper_WapperApplication_validate
        PUSH    {R3-R5,LR}
        MOVS    R4, R0
        MOVS    R5, R2
        BL      classInit
        MOVS    R0, R4
        MOVS    R1, R5
        BL      verifyDigest
        CMP     R0, #0
        BNE     loc_4B8818DE
        BLX     exit
; ---------------------------------------------------------------

loc_4B8818DE                    ; CODE XREF: Java_com_merry_wapper_Wap
        MOVS    R1, R5
        MOVS    R0, R4
        BL      decryptDex
        MOVS    R0, R4
        BL      classDestroy
        POP     {R3-R5,PC}
; End of function Java_com_merry_wapper_WapperApplication_validate
```

Static Analysis - libnsecure.so

- Exports
- Java_com_merry_wrapper_WrapperApplication_validate

```
        EXPORT Java_com_merry_wapper_WapperApplication_validate
Java_com_merry_wapper_WapperApplication_validate
        PUSH   {R3-R5,LR}
        MOVS   R4, R0
        MOVS   R5, R2
        BL     classInit
        MOVS   R0, R4
        MOVS   R1, R5
        BL     verifyDigest
        CMP    R0, #0
        BNE    loc_4B8818DE
        BLX    exit
; ---------------------------------------------------------------

loc_4B8818DE                    ; CODE XREF: Java_com_merry_wapper_Wap
        MOVS   R1, R5
        MOVS   R0, R4
        BL     decryptDex
        MOVS   R0, R4
        BL     classDestroy
        POP    {R3-R5,PC}
; End of function Java_com_merry_wapper_WapperApplication_validate
```

Pangxie

Unpacking

- **verifyDigest()**
  - Reads asset file **diest**

Unpacking

- **verifyDigest()**
  - Reads asset file **diest**
  - Calls decryption function

```
.text:4B881D34
.text:4B881D34          EXPORT digestDecrypt
.text:4B881D34 digestDecrypt                    ; CODE XREF: verifyDigest+1EE↑p
.text:4B881D34          PUSH   {R3,LR}
.text:4B881D36          LDR    R2, =(a0123456789012 - 0x4B881D3C)
.text:4B881D38          ADD    R2, PC          "0123456789012345"  =KEY
.text:4B881D3A          BL     AESDecrypt
.text:4B881D3E          POP    {R3,PC}
.text:4B881D3E ; End of function digestDecrypt
.text:4B881D3E
```

Pangxie

Unpacking

- **verifyDigest()**
  - Reads asset file **diest**
  - Calls decryption function

```
$ openssl enc -d -aes-128-ecb -nosalt -in diest -out diest.dec -K
303132333435363738393031323334 35
```

Pangxie

Unpacking

- **verifyDigest()**
  - Reads asset file **diest**
  - Calls decryption function

```
openssl enc -d -aes-128-ecb -nosalt -in diest -out diest.dec -K
303132333435363738393031323334 35
```

Decrypted 'diest'

- MANIFEST.MF
- $PakageName$ == Context.getPackageName()?

Static Analysis - libnsecure.so

- Exports
- Java_com_merry_wrapper_WrapperApplication_validate

```
        EXPORT Java_com_merry_wapper_WapperApplication_validate
Java_com_merry_wapper_WapperApplication_validate
        PUSH   {R3-R5,LR}
        MOVS   R4, R0
        MOVS   R5, R2
        BL     classInit
        MOVS   R0, R4
        MOVS   R1, R5
        BL     verifyDigest
        CMP    R0, #0
        BNE    loc_4B8818DE
        BLX    exit
; ---------------------------------------------------------------

loc_4B8818DE                    ; CODE XREF: Java_com_merry_wapper_Wap
        MOVS   R1, R5
        MOVS   R0, R4
        BL     decryptDex
        MOVS   R0, R4
        BL     classDestroy
        POP    {R3-R5,PC}
; End of function Java_com_merry_wapper_WapperApplication_validate
```

Pangxie

Unpacking

- **verifyDigest()**
- **decryptDex()**
  - Reads asset file **clex**

Unpacking

- **verifyDigest()**
- **decryptDex()**
  - Reads asset file **clex**
  - Calls decryption function

```
        EXPORT dexDecrypt
dexDecrypt                  ; CODE XREF: decryptDex+68↑p
        PUSH   {R3-R7,LR}
        MOVS   R5, R0       ; Read Pointer to Buffer
        MOVS   R6, R1       ; Read Size of 'clex'
        MOVS   R3, #0
        MOVS   R2, #0x58    ; XOR key
        B      loc_4B881938

my_DecryptionFn             ; CODE XREF: dexDecrypt+16↓j
        LDRB   R1, [R5,R3]  ; Read Byte from Buffer
        EORS   R1, R2       ; XOR with key value
        STRB   R1, [R5,R3]  ; Store in Buffer
        ADDS   R3, #1

loc_4B881938                ; CODE XREF: dexDecrypt+A↑j
        CMP    R3, R6
        BLT    my_DecryptionFn
        LDR    R3, =(cpakageName_ptr - 0x4B881942)
        ADD    R3, PC ; cpakageName_ptr
```

Pangxie

Unpacking

- **verifyDigest()**
- **decryptDex()**

Decrypted 'clex'

- JAR/APK containing original DEX
- Saved as /data/data/[pkg_name]/app_dex/classes.jar
- Loaded using DexClassLoader

Pangxie

Analyst Friendly

- Entirely analyzed using **only Static Analysis**
- **Symbol Table intact** in ELF shared Library
- 'Helpful' Export Names
- **'Simple' encryption**
- No heavy obfuscation

LIAPP

```
00001160  8d eb 6b 46 bf e2 2b 0e  13 f5 5e 93 85 9c 1f da  |..kF..+...^.....|
00001170  5c c5 e8 1f 15 cc d2 86  78 13 07 1e 4d f4 63 c7  |\.......x...M.c.|
00001180  89 61 80 06 96 46 59 0d  33 4f ad 0c 1b aa 0e 85  |.a...FY.3O......|
00001190  61 08 a1 9e 99 5e d9 19  fc 81 be 54 55 d5 92 8d  |a....^.....TU...|
000011a0  fb 2f 24 c2 b9 26 0d 02  22 9a 8e aa 76 2e 1c 8f  |./$..&.."...v...|
000011b0  b4 03 1d 7d 12 3f 0f 6e  54 37 57 c6 4b 76 36 cf  |...}.?.nT7W.Kv6.|
000011c0  8d 45 94 e9 7c 47 be da  55 c7 63 c0 99 ce 45 77  |.E..|G..U.c...Ew|
000011d0  43 38 ff 2e 50 89 c0 92  1c f2 ae af af 96 44 6f  |C8..P.........Do|
000011e0  49 96 c2 61 66 c6 40 e8  fe 6a 44 2c 54 88 e7 d8  |I..af.@..jD,T...|
000011f0  17 aa c1 92 7e 9b 4c f8  05 67 7e 19 53 0c 06 0f  |....~.L..g~.S...|
00001200  cf b4 0d 33 46 8e da 73  49 e0 05 ef 9d 9e fc 0c  |...3F..sI.......|
00001210  a3 93 c5 b5 38 75 96 f0  22 43 7f 5c f8 da 12 b6  |....8u.."C.\....|
00001220  de 67 3b 6b 02 b3 70 4a  90 18 04 86 03 20 01 1e  |.g;k..pJ..... ..|
*
00001240  76 29 3c 26 e6 ee 85 32  02 11 e5 a4 a4 1f 3a 78  |v)<&...2......:x|
00001250  36 42 f1 5a 24 86 1f 9e  33 35 ff 82 b3 d6 d5 2e  |6B.Z$...35......|
00001260  ea b6 f6 20 c4 b2 44 8d  1f 90 c0 f4 a8 d2 2f f7  |... ..D...../.|
000012e0  f1 ec f9 9c fb e6 2e a5  66 97 71 99 f4 6e c3 88  |........f.q..n..|
000012f0  8b 3a bf 33 8e 67 ea 84  af ab f8 14 56 1d 40 82  |.:.3.g......V.@.|
00001300  ef 28 b7 3c 8d c1 a0 08  b7 be 8b fd a2 86 96 73  |.(.<...........s|
00001310  b2 c3 a7 58 07 9a 9c 81  07 f9 4a b5 94 92 2b 67  |...X......J...+g|
00001320  04 b7 46 ae ef ab 9a 17  d4 79 ed 97 d5 95 1e c2  |..F......y......|
00001330  e2 74 73 f4 0a 33 ca c2  4e 10 65 bd b2 09 df 25  |.ts..3..N.e....%|
00001340  64 1b ec dd b8 ab 1e 12  50 a3 a4 65 17 86 15 6b  |d.......P..e...k|
00001350  8f 59 1b 80 4a c7 d8 69  bb 41 48 d2 e8 e3 63 8a  |.Y..J..i.AH...c.|
00001360  85 a7 1c 32 55 24 de d1  e2 84 cc b9 1e 7d 91 de  |...2U$.......}..|
00001370  a5 55 9f 5e 0b 9a c8 3e  89 64 21 61 62 f6 d6 d6  |.U.^...>.d!ab...|
00001380  df 6f cf 51 ee 1d 9b c8  32 15 2b d9 42 c5 53 91  |.o.Q....2.+.B.S.|
00001390  01 09 2a c2 9e 1e 85 93  59 f9 e6 cf 18 7d 20 29  |..*.....Y....} )|
000013a0  4b b6 1c d8 cb f2 7f 66  54 aa a3 84 91 45 f7 95  |K......fT....E..|
000013b0  5e f5 fa f6 fc db 05 60  fd d5 6f 1f 6e bc 1a fe  |^......`..o.n...|
000013c0  1a 17 83 0e b6 9c 17 0c  84 ad 3c 2d 03 ff 1a 82  |..........<-....|
000013d0  93 e2 77 ca 55 ed d0 ba  6e f0 58 08 bf 09 77 8b  |..w.U...n.X...w.|
000013e0  e1 dd 6b 6d 77 27 1e d5  22 4b 4c b5 66 95 79 b6  |..kmw'.."KL.f.y.|
000013f0  0e 3a 48 71 28 81 d6 11  74 48 5e a1 f3 e4 e9 27  |.:Hq(...tH^....'|
00001400  6d 8e 44 52 e4 bb c4 42  a5 ba 9e c7 68 1e f5 ab  |m.DR...B....h...|
00001410  1a 17 83 0e b6 9c 17 0c  84 ad 3c 2d 03 ff 1a 82  |..........<-....|
00001420  ff c9 33 80 75 3b 30 33  ce bc 00 cc 0c c7 da 4c  |..3.u;03.......L|
00001430  d4 21 47 c5 af 03 de e0  8a 2e 8c 91 70 d8 db da  |.!G.........p...|
00001440  48 f9 9e 18 d8 e8 26 b9  f7 aa 0e 47 01 5c d2 43  |H.....&....G.\.C|
00001450  fd 57 0f ca ee cc c3 df  b2 59 95 15 31 55 d0 51  |.W.......Y..1U.Q|
00001460  04 b7 46 ae ef ab 9a 17  d4 79 ed 97 d5 95 1e c2  |..F......y......|
00001470  4c 8d 75 fc 6c dd 36 f7  d9 66 a5 ad 66 8b e1 8d  |L.u.l.6..f..f...|
00001480  c2 70 23 47 03 b7 9d 88  92 d2 59 09 b3 c0 68 b8  |.p#G......Y...h.|
00001490  21 60 5c 10 a9 8e 7b f0  43 32 93 27 7f 18 82 53  |!`\...{.C2.'...S|
```

```
00001150  30 00 41 28 00 00 00 61  65 61 62 69 00 01 1e 00  |0.A(...aeabi....|
00001160  00 00 05 35 54 45 00 06  04 08 01 09 01 12 04 14  |...5TE..........|
00001170  01 15 01 17 03 18 01 19  01 1a 02 00 2e 73 68 73  |.............shs|
00001180  74 72 74 61 62 00 2e 69  6e 74 65 72 70 00 2e 68  |trtab..interp..h|
00001190  61 73 68 00 2e 64 79 6e  73 79 6d 00 2e 64 79 6e  |ash..dynsym..dyn|
000011a0  73 74 72 00 2e 72 65 6c  2e 70 6c 74 00 2e 74 65  |str..rel.plt..te|
000011b0  78 74 00 2e 72 6f 64 61  74 61 00 2e 70 72 65 69  |xt..rodata..prei|
000011c0  6e 69 74 5f 61 72 72 61  79 00 2e 69 6e 69 74 5f  |nit_array..init_|
000011d0  61 72 72 61 79 00 2e 66  69 6e 69 5f 61 72 72 61  |array..fini_arra|
000011e0  79 00 2e 63 74 6f 72 73  00 2e 64 79 6e 61 6d 69  |y..ctors..dynami|
000011f0  63 00 2e 67 6f 74 00 2e  62 73 73 00 2e 63 6f 6d  |c..got..bss..com|
00001200  6d 65 6e 74 00 2e 41 52  4d 2e 61 74 74 72 69 62  |ment..ARM.attrib|
00001210  75 74 65 73 00 00 00 00  00 00 00 00 00 00 00 00  |utes............|
00001220  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00001240  0b 00 00 00 01 00 00 00  02 00 00 00 d4 80 00 00  |................|
00001250  d4 00 00 00 13 00 00 00  00 00 00 00 00 00 00 00  |................|
000012d0  00 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00  |................|
000012e0  29 00 00 00 09 00 00 00  02 00 00 00 bc 84 00 00  |)...............|
000012f0  bc 04 00 00 98 00 00 00  03 00 00 00 06 00 00 00  |................|
00001300  04 00 00 00 08 00 00 00  2d 00 00 00 01 00 00 00  |........-.......|
00001310  06 00 00 00 54 85 00 00  54 05 00 00 f8 00 00 00  |....T...T.......|
00001320  00 00 00 00 00 00 00 00  04 00 00 00 04 00 00 00  |................|
00001330  32 00 00 00 01 00 00 00  06 00 00 00 50 86 00 00  |2...........P...|
00001340  50 06 00 00 e8 02 00 00  00 00 00 00 00 00 00 00  |P...............|
00001350  10 00 00 00 00 00 00 00  38 00 00 00 01 00 00 00  |........8.......|
00001360  32 00 00 00 38 89 00 00  38 09 00 00 e0 02 00 00  |2...8...8.......|
00001370  00 00 00 00 00 00 00 00  04 00 00 00 01 00 00 00  |................|
00001380  40 00 00 00 10 00 00 00  03 00 00 00 90 00 00 00  |@...............|
00001390  00 10 00 00 08 00 00 00  00 00 00 00 00 00 00 00  |................|
000013a0  01 00 00 00 00 00 00 00  4f 00 00 00 0e 00 00 00  |........O.......|
000013b0  03 00 00 00 08 90 00 00  08 10 00 00 08 00 00 00  |................|
000013c0  00 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00  |................|
000013d0  5b 00 00 00 0f 00 00 00  03 00 00 00 10 90 00 00  |[...............|
000013e0  10 10 00 00 08 00 00 00  00 00 00 00 00 00 00 00  |................|
000013f0  01 00 00 00 00 00 00 00  67 00 00 00 01 00 00 00  |........g.......|
00001400  03 00 00 00 18 90 00 00  18 10 00 00 08 00 00 00  |................|
00001410  00 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00  |................|
00001420  6e 00 00 00 06 00 00 00  03 00 00 00 20 90 00 00  |n..............  ...|
00001430  20 10 00 00 c8 00 00 00  04 00 00 00 00 00 00 00  |  ..............|
00001440  04 00 00 00 08 00 00 00  77 00 00 00 01 00 00 00  |........w.......|
00001450  03 00 00 00 e8 90 00 00  e8 10 00 00 58 00 00 00  |............X...|
00001460  00 00 00 00 00 00 00 00  04 00 00 00 04 00 00 00  |................|
00001470  7c 00 00 00 08 00 00 00  03 00 00 00 40 91 00 00  |||...........@...|
00001480  40 11 00 00 10 00 00 00  00 00 00 00 00 00 00 00  |@...............|
```

LIAPP

Static Analysis

- 'com.lockincomp.liapp.LiappCommon'

```
<?xml version="1.0" encoding="utf-8"?>
<manifest package="com.fortiguard.demo.mobclix.myage" android:versionCode="1"
android:versionName="1.0"
  xmlns:android="http://schemas.android.com/apk/res/android">
    <application android:label="@string/app_name" android:icon="@drawable/logo
    " android:name="com.lockincomp.liapp.LiappCommon">
        <activity android:label="@string/app_name" android:name="MyAge">
```

LIAPP

Static Analysis

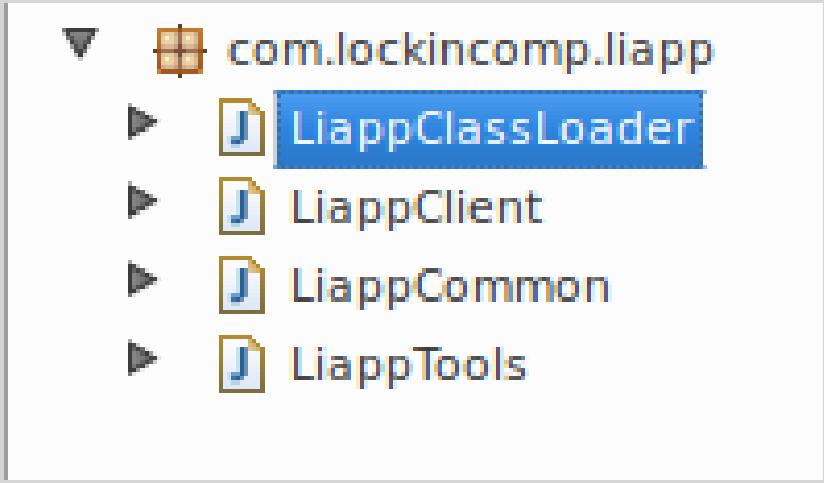
- 'com.lockincomp.liapp.LiappCommon'
- LiappCommon.class

```
public void onCreate()
{
  super.onCreate();
  if (!bInitSuccess)
    LiappCommonFinish();
  m_CC = this;
  if (CustomApplication != null)
  {
    LiappClient.LCA1(CustomApplication, getBaseContext());
    CustomApplication.onCreate();
    LiappClient.LCA3(this, CustomApplication);
  }
}
```

LIAPP

Static Analysis

- 'com.lockincomp.liapp.LiappCommon'
- LiappCommon.class
- Other classes



LIAPP

Static Analysis

- 'com.lockincomp.liapp.LiappCommon'
- LiappCommon.class
- Other classes - DexClassLoader
- Additional files in packed APK

```
├── AndroidManifest.xml
├── apktool.yml
├── assets
│   ├── LIAPPClient.sc
│   ├── LIAPPClient_x86.sc
│   ├── LIAPPEgg.jar
│   ├── LIAPPEgg.re
│   ├── LIAPPEgg.sc
│   └── LIAPPEgg_x86.sc
├── res
```

LIAPP

Dynamic Analysis

- Install and run on emulator
- gdbserver - Attach to process
- gdb client - Dump memory area of interest

```
00001160  8d eb 6b 46 bf e2 2b 0e  13 f5 5e 93 85 9c 1f da  |..kF..+...^.....|
00001170  5c c5 e8 1f 15 cc d2 86  78 13 07 1e 4d f4 63 c7  |\.......x...M.c.|
00001180  89 61 80 06 96 46 59 0d  33 4f ad 0c 1b aa 0e 85  |.a...FY.3O......|
00001190  61 08 a1 9e 99 5e d9 19  fc 81 be 54 55 d5 92 8d  |a....^.....TU...|
000011a0  fb 2f 24 c2 b9 26 0d 02  22 9a 8e aa 76 2e 1c 8f  |./$..&.."...v...|
000011b0  b4 03 1d 7d 12 3f 0f 6e  54 37 57 c6 4b 76 36 cf  |...}.?.nT7W.Kv6.|
000011c0  8d 45 94 e9 7c 47 be da  55 c7 63 c0 99 ce 45 77  |.E..|G..U.c...Ew|
000011d0  43 38 ff 2e 50 89 c0 92  1c f2 ae af af 96 44 6f  |C8..P.........Do|
000011e0  49 96 c2 61 66 c6 40 e8  fe 6a 44 2c 54 88 e7 d8  |I..af.@..jD,T...|
000011f0  17 aa c1 92 7e 9b 4c f8  05 67 7e 19 53 0c 06 0f  |....~.L..g~.S...|
00001200  cf b4 0d 33 46 8e da 73  49 e0 05 ef 9d 9e fc 0c  |...3F..sI.......|
00001210  a3 93 c5 b5 38 75 96 f0  22 43 7f 5c f8 da 12 b6  |....8u.."C.\....|
00001220  de 67 3b 6b 02 b3 70 4a  90 18 04 86 03 20 01 1e  |.g;k..pJ..... ..|
*
00001240  76 29 3c 26 e6 ee 85 32  02 11 e5 a4 a4 1f 3a 78  |v)<&...2......:x|
00001250  36 42 f1 5a 24 86 1f 9e  33 35 ff 82 b3 d6 d5 2e  |6B.Z$...35......|
00001260  ea b6 f6 20 c4 b2 44 8d  1f 90 c0 f4 a8 d2 2f f7  |... ..D...../.|
00001
0000
0000
0000
0000
0000
0000
000012c
000012e0  f1 ec f9 9c fb e6 2e a5  66 97 71 99 f4 6e c3 88  |........f.q..n..|
000012f0  8b 3a bf 33 8e 67 ea 84  af ab f8 14 56 1d 40 82  |.:.3.g......V.@.|
00001300  ef 28 b7 3c 8d c1 a0 08  b7 be 8b fd a2 86 96 73  |.(.<...........s|
00001310  b2 c3 a7 58 07 9a 9c 81  07 f9 4a b5 94 92 2b 67  |...X......J...+g|
00001320  04 b7 46 ae ef ab 9a 17  d4 79 ed 97 d5 95 1e c2  |..F......y......|
00001330  e2 74 73 f4 0a 33 ca c2  4e 10 65 bd b2 09 df 25  |.ts..3..N.e....%|
00001340  64 1b ec dd b8 ab 1e 12  50 a3 a4 65 17 86 15 6b  |d.......P..e...k|
00001350  8f 59 1b 80 4a c7 d8 69  bb 41 48 d2 e8 e3 63 8a  |.Y..J..i.AH...c.|
00001360  85 a7 1c 32 55 24 de d1  e2 84 cc b9 1e 7d 91 de  |...2U$.......}..|
00001370  a5 55 9f 5e 0b 9a c8 3e  89 64 21 61 62 f6 d6 d6  |.U.^...>.d!ab...|
00001380  df 6f cf 51 ee 1d 9b c8  32 15 2b d9 42 c5 53 91  |.o.Q....2.+.B.S.|
00001390  01 09 2a c2 9e 1e 85 93  59 f9 e6 cf 18 7d 20 29  |..*.....Y....} )|
000013a0  4b b6 1c d8 cb f2 7f 66  54 aa a3 84 91 45 f7 95  |K......fT....E..|
000013b0  5e f5 fa f6 fc db 05 60  fd d5 6f 1f 6e bc 1a fe  |^......`..o.n...|
000013c0  1a 17 83 0e b6 9c 17 0c  84 ad 3c 2d 03 ff 1a 82  |..........<-....|
000013d0  93 e2 77 ca 55 ed d0 ba  6e f0 58 08 bf 09 77 8b  |..w.U...n.X...w.|
000013e0  e1 dd 6b 6d 77 27 1e d5  22 4b 4c b5 66 95 79 b6  |..kmw'.."KL.f.y.|
000013f0  0e 3a 48 71 28 81 d6 11  74 48 5e a1 f3 e4 e9 27  |.:Hq(...tH^....'|
00001400  6d 8e 44 52 e4 bb c4 42  a5 ba 9e c7 68 1e f5 ab  |m.DR...B....h...|
00001410  1a 17 83 0e b6 9c 17 0c  84 ad 3c 2d 03 ff 1a 82  |..........<-....|
00001420  ff c9 33 80 75 3b 30 33  ce bc 00 cc 0c c7 da 4c  |..3.u;03.......L|
00001430  d4 21 47 c5 af 03 de e0  8a 2e 8c 91 70 d8 db da  |.!G.........p...|
00001440  48 f9 9e 18 d8 e8 26 b9  f7 aa 0e 47 01 5c d2 43  |H.....&....G.\.C|
00001450  fd 57 0f ca ee cc c3 df  b2 59 95 15 31 55 d0 51  |.W.......Y..1U.Q|
00001460  04 b7 46 ae ef ab 9a 17  d4 79 ed 97 d5 95 1e c2  |..F......y......|
00001470  4c 8d 75 fc 6c dd 36 f7  d9 66 a5 ad 66 8b e1 8d  |L.u.l.6..f..f...|
00001480  c2 70 23 47 03 b7 9d 88  92 d2 59 09 b3 c0 68 b8  |.p#G......Y...h.|
00001490  21 60 5c 10 a9 8e 7b f0  43 32 93 27 7f 18 82 53  |!`\...{.C2.'...S|
```

```
00001150  30 00 41 28 00 00 00 61  65 61 62 69 00 01 1e 00  |0.A(...aeabi....|
00001160  00 00 05 35 54 45 00 06  04 08 01 09 01 12 04 14  |...5TE..........|
00001170  01 15 01 17 03 18 01 19  01 1a 02 00 2e 73 68 73  |.............shs|
00001180  74 72 74 61 62 00 2e 69  6e 74 65 72 70 00 2e 68  |trtab..interp..h|
00001190  61 73 68 00 2e 64 79 6e  73 79 6d 00 2e 64 79 6e  |ash..dynsym..dyn|
000011a0  73 74 72 00 2e 72 65 6c  2e 70 6c 74 00 2e 74 65  |str..rel.plt..te|
000011b0  78 74 00 2e 72 6f 64 61  74 61 00 2e 70 72 65 69  |xt..rodata..prei|
000011c0  6e 69 74 5f 61 72 72 61  79 00 2e 69 6e 69 74 5f  |nit_array..init_|
000011d0  61 72 72 61 79 00 2e 66  69 6e 69 5f 61 72 72 61  |array..fini_arra|
000011e0  79 00 2e 63 74 6f 72 73  00 2e 64 79 6e 61 6d 69  |y..ctors..dynami|
000011f0  63 00 2e 67 6f 74 00 2e  62 73 73 00 2e 63 6f 6d  |c..got..bss..com|
00001200  6d 65 6e 74 00 2e 41 52  4d 2e 61 74 74 72 69 62  |ment..ARM.attrib|
00001210  75 74 65 73 00 00 00 00  00 00 00 00 00 00 00 00  |utes............|
00001220  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00001240  0b 00 00 00 01 00 00 00  02 00 00 00 d4 80 00 00  |................|
00001250  d4 00 00 00 13 00 00 00  00 00 00 00 00 00 00 00  |................|
000012d0  00 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00  |................|
000012e0  29 00 00 00 09 00 00 00  02 00 00 00 bc 84 00 00  |)...............|
000012f0  bc 04 00 00 98 00 00 00  03 00 00 00 06 00 00 00  |................|
00001300  04 00 00 00 08 00 00 00  2d 00 00 00 01 00 00 00  |........-.......|
00001310  06 00 00 00 54 85 00 00  54 05 00 00 f8 00 00 00  |....T...T.......|
00001320  00 00 00 00 00 00 00 00  04 00 00 00 04 00 00 00  |................|
00001330  32 00 00 00 01 00 00 00  06 00 00 00 50 86 00 00  |2...........P...|
00001340  50 06 00 00 e8 02 00 00  00 00 00 00 00 00 00 00  |P...............|
00001350  10 00 00 00 00 00 00 00  38 00 00 00 01 00 00 00  |........8.......|
00001360  32 00 00 00 38 89 00 00  38 09 00 00 e0 02 00 00  |2...8...8.......|
00001370  00 00 00 00 00 00 00 00  04 00 00 00 01 00 00 00  |................|
00001380  40 00 00 00 10 00 00 00  03 00 00 00 90 00 00 00  |@...............|
00001390  00 10 00 00 08 00 00 00  00 00 00 00 00 00 00 00  |................|
000013a0  01 00 00 00 00 00 00 00  4f 00 00 00 0e 00 00 00  |........O.......|
000013b0  03 00 00 00 08 90 00 00  08 10 00 00 08 00 00 00  |................|
000013c0  00 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00  |................|
000013d0  5b 00 00 00 0f 00 00 00  03 00 00 00 10 90 00 00  |[...............|
000013e0  10 10 00 00 08 00 00 00  00 00 00 00 00 00 00 00  |................|
000013f0  01 00 00 00 00 00 00 00  67 00 00 00 01 00 00 00  |........g.......|
00001400  03 00 00 00 18 90 00 00  18 10 00 00 08 00 00 00  |................|
00001410  00 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00  |................|
00001420  6e 00 00 00 06 00 00 00  03 00 00 00 20 90 00 00  |n..............  ...|
00001430  20 10 00 00 c8 00 00 00  04 00 00 00 00 00 00 00  | ...............|
00001440  04 00 00 00 08 00 00 00  77 00 00 00 01 00 00 00  |........w.......|
00001450  03 00 00 00 e8 90 00 00  e8 10 00 00 58 00 00 00  |............X...|
00001460  00 00 00 00 00 00 00 00  04 00 00 00 04 00 00 00  |................|
00001470  7c 00 00 00 08 00 00 00  03 00 00 00 40 91 00 00  |||...........@...|
00001480  40 11 00 00 10 00 00 00  00 00 00 00 00 00 00 00  |@...............|
```

DEMO

LIAPP

Unpacking

Memory Dump = Optimized DEX

- baksmali.jar : odex ->smali
- smali.jar : smali ->dex

LIAPP: Level 2

Anti-VM

- Emulator detection
- android.os.Debug.isDebuggerConnected()

LIAPP: Level 2

Anti-VM

- Emulator detection
- android.os.Debug.isDebuggerConnected()

Fix

- Run on phone and dump - Works

LIAPP: Level 2

Anti-VM

- Emulator detection
- android.os.Debug.isDebuggerConnected()

Fix

- Run on phone - Works
- Bypass Anti-VM

LIAPP: Level 2

Anti-VM

- Emulator detection
- android.os.Debug.isDebuggerConnected()

Fix

- Run on phone - Works
- Bypass Anti-VM
- Statically unpack

BANGCLE

```
00001160  8d eb 6b 46 bf e2 2b 0e  13 f5 5e 93 85 9c 1f da  |..kF..+...^.....|
00001170  5c c5 e8 1f 15 cc d2 86  78 13 07 1e 4d f4 63 c7  |\.......x...M.c.|
00001180  89 61 80 06 96 46 59 0d  33 4f ad 0c 1b aa 0e 85  |.a...FY.3O......|
00001190  61 08 a1 9e 99 5e d9 19  fc 81 be 54 55 d5 92 8d  |a....^.....TU...|
000011a0  fb 2f 24 c2 b9 26 0d 02  22 9a 8e aa 76 2e 1c 8f  |./$..&.."...v...|
000011b0  b4 03 1d 7d 12 3f 0f 6e  54 37 57 c6 4b 76 36 cf  |...}.?.nT7W.Kv6.|
000011c0  8d 45 94 e9 7c 47 be da  55 c7 63 c0 99 ce 45 77  |.E..|G..U.c...Ew|
000011d0  43 38 ff 2e 50 89 c0 92  1c f2 ae af af 96 44 6f  |C8..P.........Do|
000011e0  49 96 c2 61 66 c6 40 e8  fe 6a 44 2c 54 88 e7 d8  |I..af.@..jD,T...|
000011f0  17 aa c1 92 7e 9b 4c f8  05 67 7e 19 53 0c 06 0f  |....~.L..g~.S...|
00001200  cf b4 0d 33 46 8e da 73  49 e0 05 ef 9d 9e fc 0c  |...3F..sI.......|
00001210  a3 93 c5 b5 38 75 96 f0  22 43 7f 5c f8 da 12 b6  |....8u.."C.\....|
00001220  de 67 3b 6b 02 b3 70 4a  90 18 04 86 03 20 01 1e  |.g;k..pJ..... ..|
*
00001240  76 29 3c 26 e6 ee 85 32  02 11 e5 a4 a4 1f 3a 78  |v)<&...2......:x|
00001250  36 42 f1 5a 24 86 1f 9e  33 35 ff 82 b3 d6 d5 2e  |6B.Z$...35......|
00001260  ea b6 f6 20 c4 b2 44 8d  1f 90 c0 f4 a8 d2 2f f7  |... ..D...../.|
000012e0  f1 ec f9 9c fb e6 2e a5  66 97 71 99 f4 6e c3 88  |........f.q..n..|
000012f0  8b 3a bf 33 8e 67 ea 84  af ab f8 14 56 1d 40 82  |.:.3.g......V.@.|
00001300  ef 28 b7 3c 8d c1 a0 08  b7 be 8b fd a2 86 96 73  |.(.<...........s|
00001310  b2 c3 a7 58 07 9a 9c 81  07 f9 4a b5 94 92 2b 67  |...X......J...+g|
00001320  04 b7 46 ae ef ab 9a 17  d4 79 ed 97 d5 95 1e c2  |..F......y......|
00001330  e2 74 73 f4 0a 33 ca c2  4e 10 65 bd b2 09 df 25  |.ts..3..N.e....%|
00001340  64 1b ec dd b8 ab 1e 12  50 a3 a4 65 17 86 15 6b  |d.......P..e...k|
00001350  8f 59 1b 80 4a c7 d8 69  bb 41 48 d2 e8 e3 63 8a  |.Y..J..i.AH...c.|
00001360  85 a7 1c 32 55 24 de d1  e2 84 cc b9 1e 7d 91 de  |...2U$.......}..|
00001370  a5 55 9f 5e 0b 9a c8 3e  89 64 21 61 62 f6 d6 d6  |.U.^...>.d!ab...|
00001380  df 6f cf 51 ee 1d 9b c8  32 15 2b d9 42 c5 53 91  |.o.Q....2.+.B.S.|
00001390  01 09 2a c2 9e 1e 85 93  59 f9 e6 cf 18 7d 20 29  |..*.....Y....} )|
000013a0  4b b6 1c d8 cb f2 7f 66  54 aa a3 84 91 45 f7 95  |K......fT....E..|
000013b0  5e f5 fa f6 fc db 05 60  fd d5 6f 1f 6e bc 1a fe  |^......`..o.n...|
000013c0  1a 17 83 0e b6 9c 17 0c  84 ad 3c 2d 03 ff 1a 82  |..........<-....|
000013d0  93 e2 77 ca 55 ed d0 ba  6e f0 58 08 bf 09 77 8b  |..w.U...n.X...w.|
000013e0  e1 dd 6b 6d 77 27 1e d5  22 4b 4c b5 66 95 79 b6  |..kmw'.."KL.f.y.|
000013f0  0e 3a 48 71 28 81 d6 11  74 48 5e a1 f3 e4 e9 27  |.:Hq(...tH^....'|
00001400  6d 8e 44 52 e4 bb c4 42  a5 ba 9e c7 68 1e f5 ab  |m.DR...B....h...|
00001410  1a 17 83 0e b6 9c 17 0c  84 ad 3c 2d 03 ff 1a 82  |..........<-....|
00001420  ff c9 33 80 75 3b 30 33  ce bc 00 cc 0c c7 da 4c  |..3.u;03.......L|
00001430  d4 21 47 c5 af 03 de e0  8a 2e 8c 91 70 d8 db da  |.!G.........p...|
00001440  48 f9 9e 18 d8 e8 26 b9  f7 aa 0e 47 01 5c d2 43  |H.....&....G.\.C|
00001450  fd 57 0f ca ee cc c3 df  b2 59 95 15 31 55 d0 51  |.W.......Y..1U.Q|
00001460  04 b7 46 ae ef ab 9a 17  d4 79 ed 97 d5 95 1e c2  |..F......y......|
00001470  4c 8d 75 fc 6c dd 36 f7  d9 66 a5 ad 66 8b e1 8d  |L.u.l.6..f..f...|
00001480  c2 70 23 47 03 b7 9d 88  92 d2 59 09 b3 c0 68 b8  |.p#G......Y...h.|
00001490  21 60 5c 10 a9 8e 7b f0  43 32 93 27 7f 18 82 53  |!`\...{.C2.'...S|
```

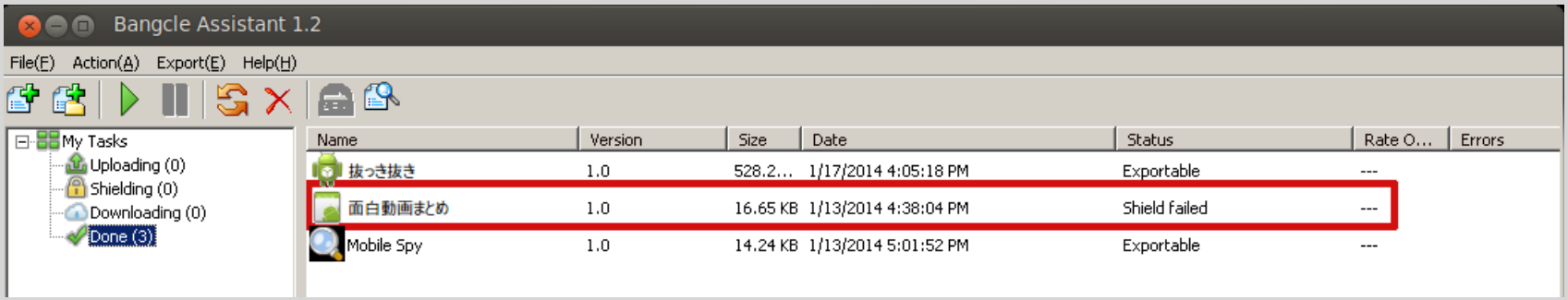
```
00001150  30 00 41 28 00 00 00 61  65 61 62 69 00 01 1e 00  |0.A(...aeabi....|
00001160  00 00 05 35 54 45 00 06  04 08 01 09 01 12 04 14  |...5TE..........|
00001170  01 15 01 17 03 18 01 19  01 1a 02 00 2e 73 68 73  |.............shs|
00001180  74 72 74 61 62 00 2e 69  6e 74 65 72 70 00 2e 68  |trtab..interp..h|
00001190  61 73 68 00 2e 64 79 6e  73 79 6d 00 2e 64 79 6e  |ash..dynsym..dyn|
000011a0  73 74 72 00 2e 72 65 6c  2e 70 6c 74 00 2e 74 65  |str..rel.plt..te|
000011b0  78 74 00 2e 72 6f 64 61  74 61 00 2e 70 72 65 69  |xt..rodata..prei|
000011c0  6e 69 74 5f 61 72 72 61  79 00 2e 69 6e 69 74 5f  |nit_array..init_|
000011d0  61 72 72 61 79 00 2e 66  69 6e 69 5f 61 72 72 61  |array..fini_arra|
000011e0  79 00 2e 63 74 6f 72 73  00 2e 64 79 6e 61 6d 69  |y..ctors..dynami|
000011f0  63 00 2e 67 6f 74 00 2e  62 73 73 00 2e 63 6f 6d  |c..got..bss..com|
00001200  6d 65 6e 74 00 2e 41 52  4d 2e 61 74 74 72 69 62  |ment..ARM.attrib|
00001210  75 74 65 73 00 00 00 00  00 00 00 00 00 00 00 00  |utes............|
00001220  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00001240  0b 00 00 00 01 00 00 00  02 00 00 00 d4 80 00 00  |................|
00001250  d4 00 00 00 13 00 00 00  00 00 00 00 00 00 00 00  |................|
000012d0  00 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00  |................|
000012e0  29 00 00 00 09 00 00 00  02 00 00 00 bc 84 00 00  |)...............|
000012f0  bc 04 00 00 98 00 00 00  03 00 00 00 06 00 00 00  |................|
00001300  04 00 00 00 08 00 00 00  2d 00 00 00 01 00 00 00  |........-.......|
00001310  06 00 00 00 54 85 00 00  54 05 00 00 f8 00 00 00  |....T...T.......|
00001320  00 00 00 00 00 00 00 00  04 00 00 00 04 00 00 00  |................|
00001330  32 00 00 00 01 00 00 00  06 00 00 00 50 86 00 00  |2...........P...|
00001340  50 06 00 00 e8 02 00 00  00 00 00 00 00 00 00 00  |P...............|
00001350  10 00 00 00 00 00 00 00  38 00 00 00 01 00 00 00  |........8.......|
00001360  32 00 00 00 38 89 00 00  38 09 00 00 e0 02 00 00  |2...8...8.......|
00001370  00 00 00 00 00 00 00 00  04 00 00 00 01 00 00 00  |................|
00001380  40 00 00 00 10 00 00 00  03 00 00 00 90 00 00 00  |@...............|
00001390  00 10 00 00 08 00 00 00  00 00 00 00 00 00 00 00  |................|
000013a0  01 00 00 00 00 00 00 00  4f 00 00 00 0e 00 00 00  |........O.......|
000013b0  03 00 00 00 08 90 00 00  08 10 00 00 08 00 00 00  |................|
000013c0  00 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00  |................|
000013d0  5b 00 00 00 0f 00 00 00  03 00 00 00 10 90 00 00  |[...............|
000013e0  10 10 00 00 08 00 00 00  00 00 00 00 00 00 00 00  |................|
000013f0  01 00 00 00 00 00 00 00  67 00 00 00 01 00 00 00  |........g.......|
00001400  03 00 00 00 18 90 00 00  18 10 00 00 08 00 00 00  |................|
00001410  00 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00  |................|
00001420  6e 00 00 00 06 00 00 00  03 00 00 00 20 90 00 00  |n..............  ...|
00001430  20 10 00 00 c8 00 00 00  04 00 00 00 00 00 00 00  |  ..............|
00001440  04 00 00 00 08 00 00 00  77 00 00 00 01 00 00 00  |........w.......|
00001450  03 00 00 00 e8 90 00 00  e8 10 00 00 58 00 00 00  |............X...|
00001460  00 00 00 00 00 00 00 00  04 00 00 00 04 00 00 00  |................|
00001470  7c 00 00 00 08 00 00 00  03 00 00 00 40 91 00 00  |||...........@...|
00001480  40 11 00 00 10 00 00 00  00 00 00 00 00 00 00 00  |@...............|
```

Bangcle

Security Enforcements by bangcle.com

- Applications are scanned before packing

Rejected Application



LIMITATION: Fails in the face of 0-days, new/unknown malware.

Bangcle

Static Analysis

- **com.secapk.wrapper.ApplicationWrapper**
- **FirstApplication** - Generic placeholder Activity
- **Native libraries** - Contain code for decrypting Dex
- **DexClassLoader** - Loads decrypted Dex

Bangcle

Resistance to Static Analysis

- Main Activity?
- Native libraries contain crux of decryption code
  - Obfuscated library export names
  - Java_com_secapk_wrapper_ACall_r1?
  - Dalvik-JNI function mapping??

.init_proc	0000FFA9
JNI_OnLoad	00007278
__FINI_ARRAY__	00020CB8
__INIT_ARRAY__	00020CB0
_init	0000BC5C
p01221BF0759EF2385B6C90AB1C269583	0000BA64
p014C8D65D9D2C854C11E605A4A92A4DA	0000E10C
p0E22CF8B99DAF2B695DFC094E7DDEF5D	00021598
p0ED08F4E91C1942E130BAE6122019015	00021E78
p10DD7C3951E520CEDC5431E9FD263803	0000B3BC

Bangcle

Resistance to Dyamic Analysis

- Can't attach to main process
- Can't stack backtrace
- ptrace hooked

Unpacking

Memory Dump

```
4b97c000-4b97e000 r--s 0006e000 1f:01 545        /data/app/com.thespyja-1.apk
4b97e000-4b983000 r--p 00000000 1f:01 615        /data/dalvik-cache/data@app@com.thespyja-1.apk@classes
.dex
4b983000-4b984000 rw-p 00000000 00:07 2650       /dev/ashmem/dalvik-aux-structure (deleted)
4b984000-4b988000 rw-p 4b984000 00:00 0
4b988000-4b98f000 r-xp 4b988000 00:00 0
4b98f000-4b991000 r--s 0006e000 1f:01 545        /data/app/com.thespyja-1.apk
4b991000-4b994000 r-xp 00000000 1f:01 605        /data/data/com.thespyja/lib/libsecexe.so
4b994000-4b9aa000 r-xp 4b994000 00:00 0
4b9aa000-4b9b1000 ---p 4b9aa000 00:00 0
4b9b1000-4b9b2000 r--p 00010000 1f:01 605        /data/data/com.thespyja/lib/libsecexe.so
4b9b2000-4b9b3000 rw-p 00011000 1f:01 605        /data/data/com.thespyja/lib/libsecexe.so
4b9b3000-4b9c1000 rwxp 4b9b3000 00:00 0
4b9c1000-4b9c2000 ---p 4b9c1000 00:00 0
4b9c2000-4bac1000 rw-p 4b9c2000 00:00 0
4bac1000-4bac2000 r-xp 4bac1000 00:00 0
4bac2000-4bac3000 ---p 4bac2000 00:00 0
4bac3000-4bbc2000 rw-p 4bac3000 00:00 0
4bbc2000-4bbc3000 ---p 4bbc2000 00:00 0
4bbc3000-4bcc2000 rw-p 4bbc3000 00:00 0
4bcc2000-4bcc3000 r--s 00000000 1f:01 520        /data/data/com.thespyja/.cache/classes.jar
4bcc3000-4bcc4000 rw-p 00000000 00:07 2677       /dev/ashmem/dalvik-aux-structure (deleted)
4bcc5000-4bcc7000 r--p 4bcc5000 00:00 0
4bcc7000-4bccb000 rw-p 4bcc7000 00:00 0
```

ApkProtect

ApkProtect

Source: http://www.apkprotect.com

ApkProtect

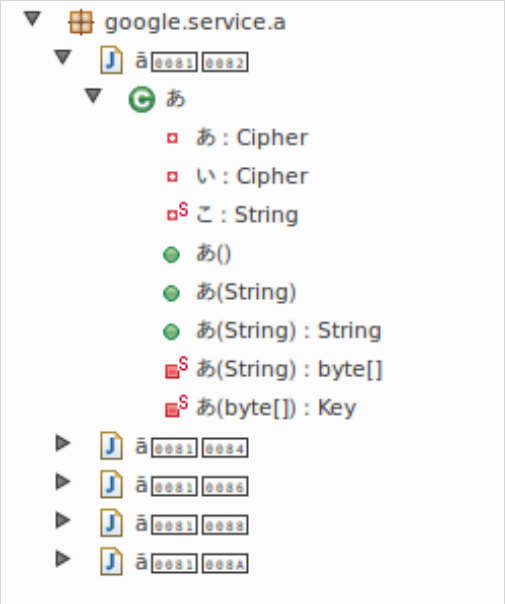
Static Analysis

- apktool Fail
- dex2jar Fail
- Unzip

ApkProtect

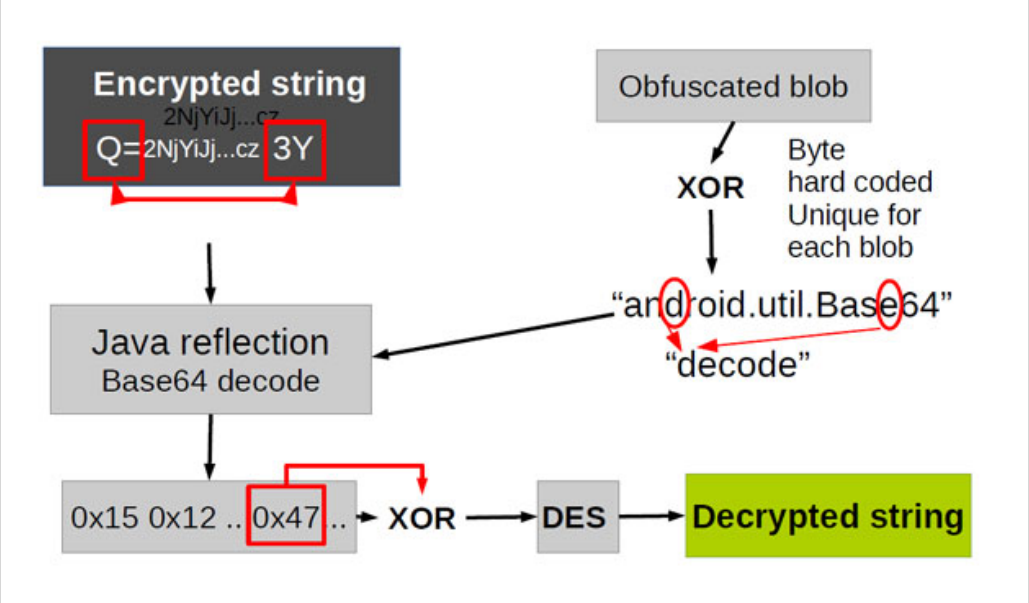
Static Analysis

- Wrapper application
- Native functions to decrypt and load code
- Strings are encrypted



ApkProtect

String decryption



- Swap first and last two bytes
- Base64 decode
- XOR with a hardcoded key (unique to each sample)
- DES decrypt with key '#safeguar'

ApkProtect

Props to

Andrubis : Analysis report reveals key

- Crypto Operations

Timestamp	Operation	Algorithm
11.220	key	DES
35, 115, 97, 102, 101, 103, 117, 97		
27.223	decryption	DES
ybbcel666.oicp.net		
27.223	decryption	DES
ybbcel777.vicp.cc		
27.223	decryption	DES
ybbcel666.oicp.net		

#safeguar

MALWARE AND DETECTION

```
00001160  8d eb 6b 46 bf e2 2b 0e  13 f5 5e 93 85 9c 1f da  |..kF..+...^.....|
00001170  5c c5 e8 1f 15 cc d2 86  78 13 07 1e 4d f4 63 c7  |\.......x...M.c.|
00001180  89 61 80 06 96 46 59 0d  33 4f ad 0c 1b aa 0e 85  |.a...FY.3O......|
00001190  61 08 a1 9e 99 5e d9 19  fc 81 be 54 55 d5 92 8d  |a....^.....TU...|
000011a0  fb 2f 24 c2 b9 26 0d 02  22 9a 8e aa 76 2e 1c 8f  |./$..&.."...v...|
000011b0  b4 03 1d 7d 12 3f 0f 6e  54 37 57 c6 4b 76 36 cf  |...}.?.nT7W.Kv6.|
000011c0  8d 45 94 e9 7c 47 be da  55 c7 63 c0 99 ce 45 77  |.E..|G..U.c...Ew|
000011d0  43 38 ff 2e 50 89 c0 92  1c f2 ae af af 96 44 6f  |C8..P.........Do|
000011e0  49 96 c2 61 66 c6 40 e8  fe 6a 44 2c 54 88 e7 d8  |I..af.@..jD,T...|
000011f0  17 aa c1 92 7e 9b 4c f8  05 67 7e 19 53 0c 06 0f  |....~.L..g~.S...|
00001200  cf b4 0d 33 46 8e da 73  49 e0 05 ef 9d 9e fc 0c  |...3F..sI.......|
00001210  a3 93 c5 b5 38 75 96 f0  22 43 7f 5c f8 da 12 b6  |....8u.."C.\....|
00001220  de 67 3b 6b 02 b3 70 4a  90 18 04 86 03 20 01 1e  |.g;k..pJ..... ..|
*
00001240  76 29 3c 26 e6 ee 85 32  02 11 e5 a4 a4 1f 3a 78  |v)<&...2......:x|
00001250  36 42 f1 5a 24 86 1f 9e  33 35 ff 82 b3 d6 d5 2e  |6B.Z$...35......|
00001260  ea b6 f6 20 c4 b2 44 8d  1f 90 c0 f4 a8 d2 2f f7  |... ..D...../.|
00001
00001
00001
00001
00001
00001
000012c
000012e0  f1 ec f9 9c fb e6 2e a5  66 97 71 99 f4 6e c3 88  |........f.q..n..|
000012f0  8b 3a bf 33 8e 67 ea 84  af ab f8 14 56 1d 40 82  |.:.3.g......V.@.|
00001300  ef 28 b7 3c 8d c1 a0 08  b7 be 8b fd a2 86 96 73  |.(.<...........s|
00001310  b2 c3 a7 58 07 9a 9c 81  07 f9 4a b5 94 92 2b 67  |...X......J...+g|
00001320  04 b7 46 ae ef ab 9a 17  d4 79 ed 97 d5 95 1e c2  |..F......y......|
00001330  e2 74 73 f4 0a 33 ca c2  4e 10 65 bd b2 09 df 25  |.ts..3..N.e....%|
00001340  64 1b ec dd b8 ab 1e 12  50 a3 a4 65 17 86 15 6b  |d.......P..e...k|
00001350  8f 59 1b 80 4a c7 d8 69  bb 41 48 d2 e8 e3 63 8a  |.Y..J..i.AH...c.|
00001360  85 a7 1c 32 55 24 de d1  e2 84 cc b9 1e 7d 91 de  |...2U$.......}..|
00001370  a5 55 9f 5e 0b 9a c8 3e  89 64 21 61 62 f6 d6 d6  |.U.^...>.d!ab...|
00001380  df 6f cf 51 ee 1d 9b c8  32 15 2b d9 42 c5 53 91  |.o.Q....2.+.B.S.|
00001390  01 09 2a c2 9e 1e 85 93  59 f9 e6 cf 18 7d 20 29  |..*.....Y....} )|
000013a0  4b b6 1c d8 cb f2 7f 66  54 aa a3 84 91 45 f7 95  |K......fT....E..|
000013b0  5e f5 fa f6 fc db 05 60  fd d5 6f 1f 6e bc 1a fe  |^......`..o.n...|
000013c0  1a 17 83 0e b6 9c 17 0c  84 ad 3c 2d 03 ff 1a 82  |..........<-....|
000013d0  93 e2 77 ca 55 ed d0 ba  6e f0 58 08 bf 09 77 8b  |..w.U...n.X...w.|
000013e0  e1 dd 6b 6d 77 27 1e d5  22 4b 4c b5 66 95 79 b6  |..kmw'.."KL.f.y.|
000013f0  0e 3a 48 71 28 81 d6 11  74 48 5e a1 f3 e4 e9 27  |.:Hq(...tH^....'|
00001400  6d 8e 44 52 e4 bb c4 42  a5 ba 9e c7 68 1e f5 ab  |m.DR...B....h...|
00001410  1a 17 83 0e b6 9c 17 0c  84 ad 3c 2d 03 ff 1a 82  |..........<-....|
00001420  ff c9 33 80 75 3b 30 33  ce bc 00 cc 0c c7 da 4c  |..3.u;03.......L|
00001430  d4 21 47 c5 af 03 de e0  8a 2e 8c 91 70 d8 db da  |.!G.........p...|
00001440  48 f9 9e 18 d8 e8 26 b9  f7 aa 0e 47 01 5c d2 43  |H.....&....G.\.C|
00001450  fd 57 0f ca ee cc c3 df  b2 59 95 15 31 55 d0 51  |.W.......Y..1U.Q|
00001460  04 b7 46 ae ef ab 9a 17  d4 79 ed 97 d5 95 1e c2  |..F......y......|
00001470  4c 8d 75 fc 6c dd 36 f7  d9 66 a5 ad 66 8b e1 8d  |L.u.l.6..f..f...|
00001480  c2 70 23 47 03 b7 9d 88  92 d2 59 09 b3 c0 68 b8  |.p#G......Y...h.|
00001490  21 60 5c 10 a9 8e 7b f0  43 32 93 27 7f 18 82 53  |!`\...{.C2.'...S|
```

```
00001150  30 00 41 28 00 00 00 61  65 61 62 69 00 01 1e 00  |0.A(...aeabi....|
00001160  00 00 05 35 54 45 00 06  04 08 01 09 01 12 04 14  |...5TE..........|
00001170  01 15 01 17 03 18 01 19  01 1a 02 00 2e 73 68 73  |.............shs|
00001180  74 72 74 61 62 00 2e 69  6e 74 65 72 70 00 2e 68  |trtab..interp..h|
00001190  61 73 68 00 2e 64 79 6e  73 79 6d 00 2e 64 79 6e  |ash..dynsym..dyn|
000011a0  73 74 72 00 2e 72 65 6c  2e 70 6c 74 00 2e 74 65  |str..rel.plt..te|
000011b0  78 74 00 2e 72 6f 64 61  74 61 00 2e 70 72 65 69  |xt..rodata..prei|
000011c0  6e 69 74 5f 61 72 72 61  79 00 2e 69 6e 69 74 5f  |nit_array..init_|
000011d0  61 72 72 61 79 00 2e 66  69 6e 69 5f 61 72 72 61  |array..fini_arra|
000011e0  79 00 2e 63 74 6f 72 73  00 2e 64 79 6e 61 6d 69  |y..ctors..dynami|
000011f0  63 00 2e 67 6f 74 00 2e  62 73 73 00 2e 63 6f 6d  |c..got..bss..com|
00001200  6d 65 6e 74 00 2e 41 52  4d 2e 61 74 74 72 69 62  |ment..ARM.attrib|
00001210  75 74 65 73 00 00 00 00  00 00 00 00 00 00 00 00  |utes............|
00001220  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00001240  0b 00 00 00 01 00 00 00  02 00 00 00 d4 80 00 00  |................|
00001250  d4 00 00 00 13 00 00 00  00 00 00 00 00 00 00 00  |................|
000012d0  00 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00  |................|
000012e0  29 00 00 00 09 00 00 00  02 00 00 00 bc 84 00 00  |)...............|
000012f0  bc 04 00 00 98 00 00 00  03 00 00 00 06 00 00 00  |................|
00001300  04 00 00 00 08 00 00 00  2d 00 00 00 01 00 00 00  |........-.......|
00001310  06 00 00 00 54 85 00 00  54 05 00 00 f8 00 00 00  |....T...T.......|
00001320  00 00 00 00 00 00 00 00  04 00 00 00 04 00 00 00  |................|
00001330  32 00 00 00 01 00 00 00  06 00 00 00 50 86 00 00  |2...........P...|
00001340  50 06 00 00 e8 02 00 00  00 00 00 00 00 00 00 00  |P...............|
00001350  10 00 00 00 00 00 00 00  38 00 00 00 01 00 00 00  |........8.......|
00001360  32 00 00 00 38 89 00 00  38 09 00 00 e0 02 00 00  |2...8...8.......|
00001370  00 00 00 00 00 00 00 00  04 00 00 00 01 00 00 00  |................|
00001380  40 00 00 00 10 00 00 00  03 00 00 00 90 00 00 00  |@...............|
00001390  00 10 00 00 08 00 00 00  00 00 00 00 00 00 00 00  |................|
000013a0  01 00 00 00 00 00 00 00  4f 00 00 00 0e 00 00 00  |........O.......|
000013b0  03 00 00 00 08 90 00 00  08 10 00 00 08 00 00 00  |................|
000013c0  00 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00  |................|
000013d0  5b 00 00 00 0f 00 00 00  03 00 00 00 10 90 00 00  |[...............|
000013e0  10 10 00 00 08 00 00 00  00 00 00 00 00 00 00 00  |................|
000013f0  01 00 00 00 00 00 00 00  67 00 00 00 01 00 00 00  |........g.......|
00001400  03 00 00 00 18 90 00 00  18 10 00 00 08 00 00 00  |................|
00001410  00 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00  |................|
00001420  6e 00 00 00 06 00 00 00  03 00 00 00 20 90 00 00  |n..............  ...|
00001430  20 10 00 00 c8 00 00 00  04 00 00 00 00 00 00 00  | ...............|
00001440  04 00 00 00 08 00 00 00  77 00 00 00 01 00 00 00  |........w.......|
00001450  03 00 00 00 e8 90 00 00  e8 10 00 00 58 00 00 00  |............X...|
00001460  00 00 00 00 00 00 00 00  04 00 00 00 04 00 00 00  |................|
00001470  7c 00 00 00 08 00 00 00  03 00 00 00 40 91 00 00  |||...........@...|
00001480  40 11 00 00 10 00 00 00  00 00 00 00 00 00 00 00  |@...............|
```

Packed malware in the wild

Known samples

- Android/SmsSend.ND!tr - ApkProtect'ed SMS sending malware
- Bangcle packed malware
  - Android/Feejar.B!tr
  - Android/FakeIns.D
  - Adware/Waps!Android etc

Detection

Visible Signs? Eg: Bangcle

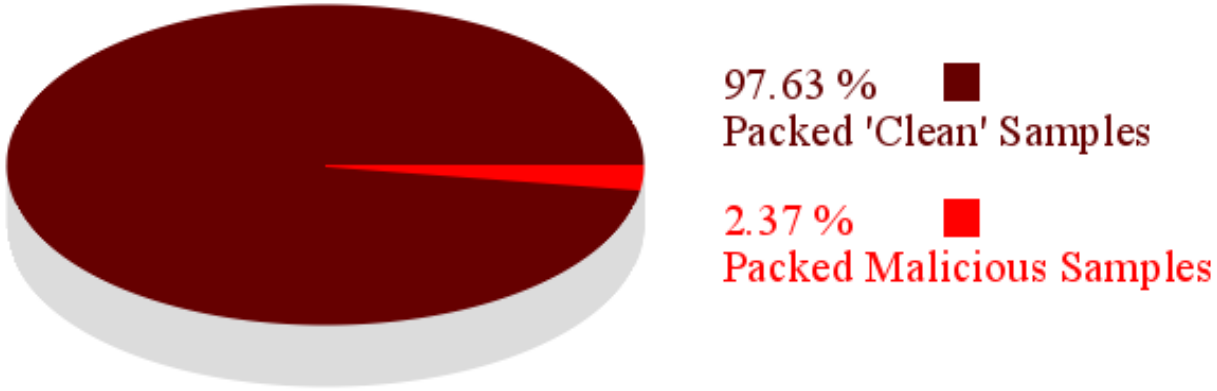
- Application name : **com.secapk.wrapper.ApplicationWrapper**
- Class names : **ACall**, **FirstApplication**
- Assets **bangcle_classes.jar**
- Native libraries **libsecexe** and **libsecmain**

Detection

Visible Signs Detection : Drawback

FALSE POSITIVES!

FP Rate = 97.63%



Detection

Challenges for Automation

- Must unpack before signing
  - Every new packer in market = >Write new unpacker
    OR
  - Behaviour based analysis i.e. Run every sample on emulator
- Time - Resource tradeoff between static & dynamic analysis

Acknowledgements

- Chinese post about Memory Dumping
- @cryptax - ApkProtect String Decryption
- @timstrazz - Pangxie Sample

Useful Links

- [PDF] Obfuscation in Android Malware Paper
- [github] Automated Unpacking Tools

The End

Thank you for listening!

Contact

- Email : rnigam[at]fortinet[dot]com
- Blog : blog.fortinet.com