Android Packers:
Separating from the pack

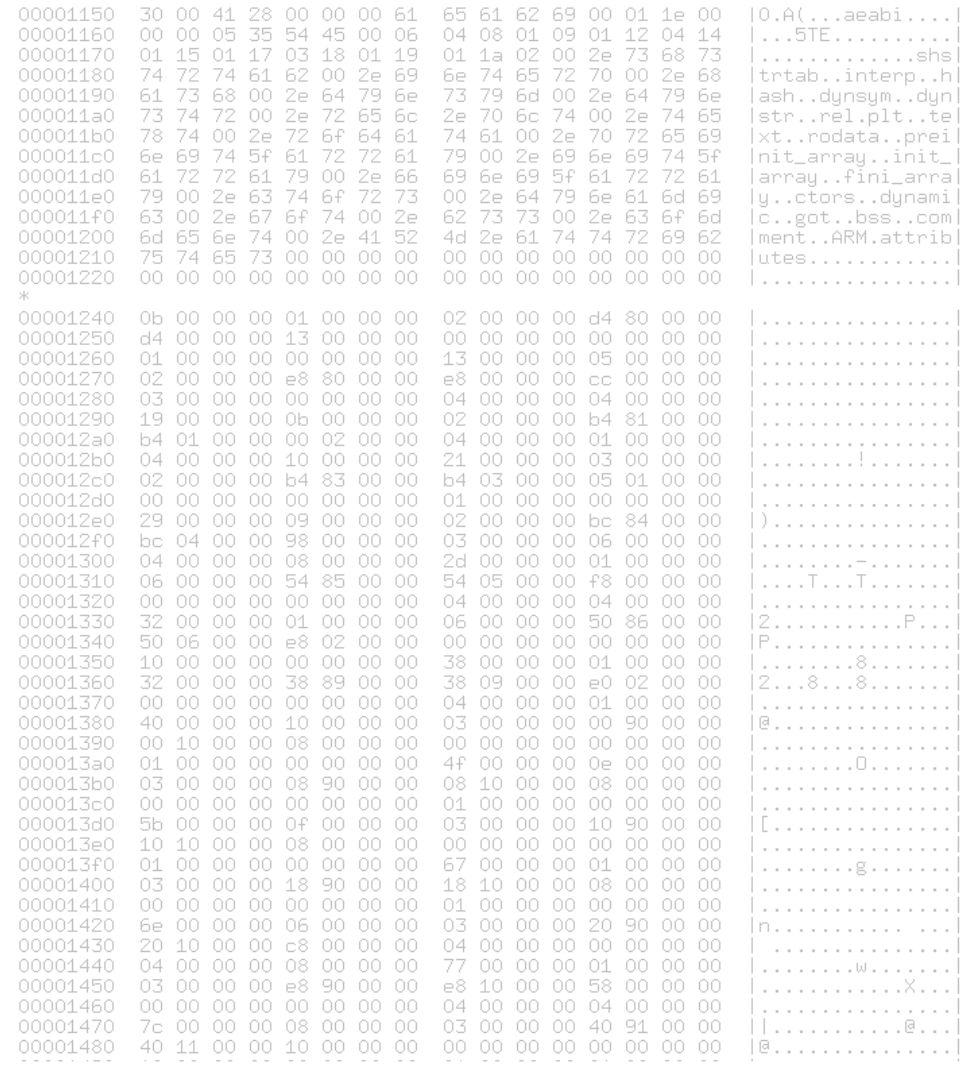
Ruchna Nigam

FortiGuard Labs,
FORTINET

Area41 - June, 2014

Today's Agenda

- What are Packers?
- Known Android Packers
- Bangcle
- Ijiami
- Packed Malware in the Wild
- Detection



Packers

What are Packers

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

Packers

Relevance

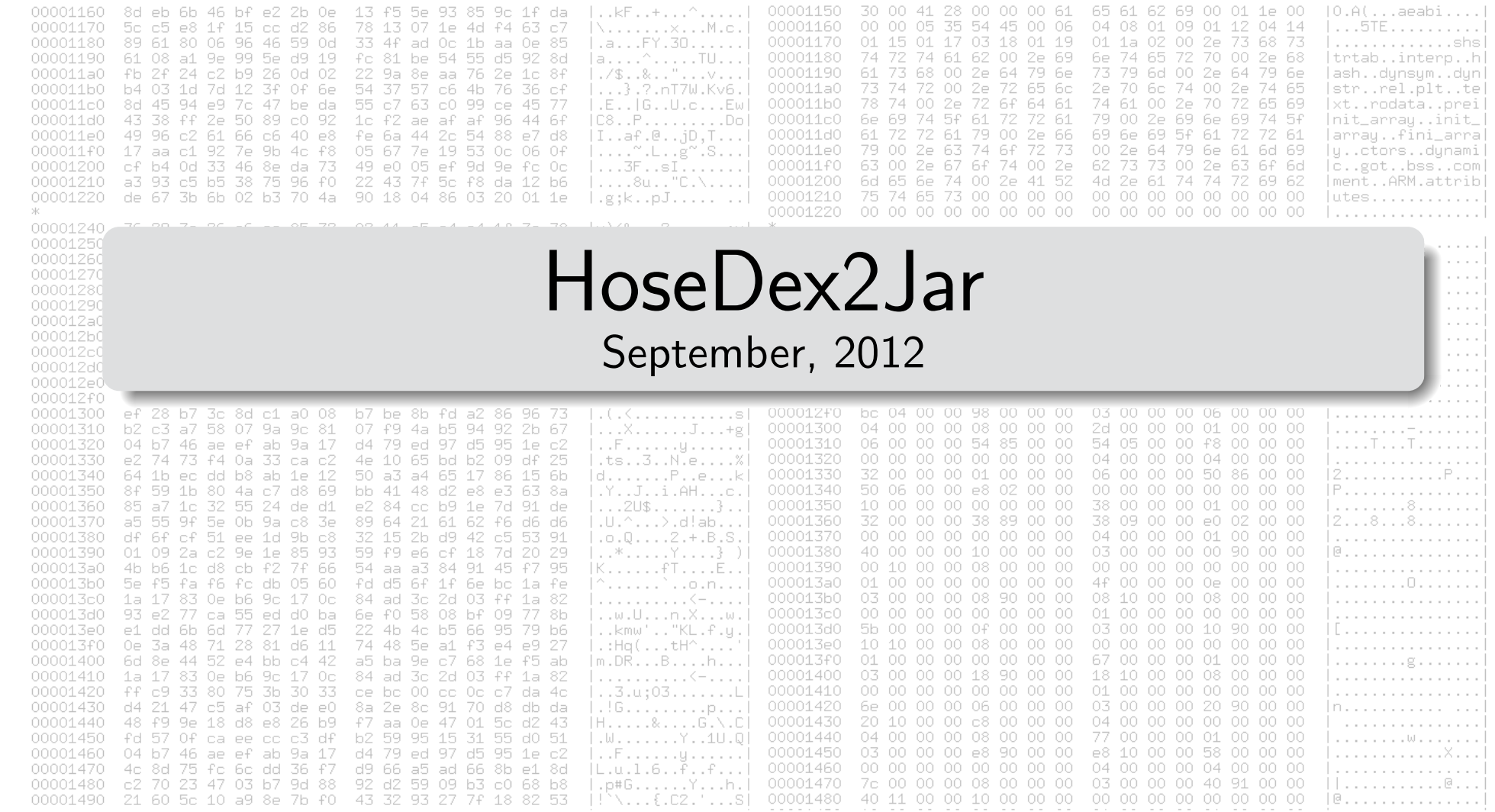
- Intended Use - Code Protection from
  - Modification
  - Piracy
  - Malicious code injection
- Flipside
  - Used on malware
  - Anti-hacker = Anti-analyst?

Android Packers

Known Android Packers[1]

- HoseDex2Jar
- ApkProtect
- Bangcle
- Ijiami

As of May, 2014



HoseDex2Jar

September, 2012

HoseDex2Jar

How does it work?

- 0x70 byte Dex header size not enforced
- Original Dex encrypted
- Added at the end of Dex header

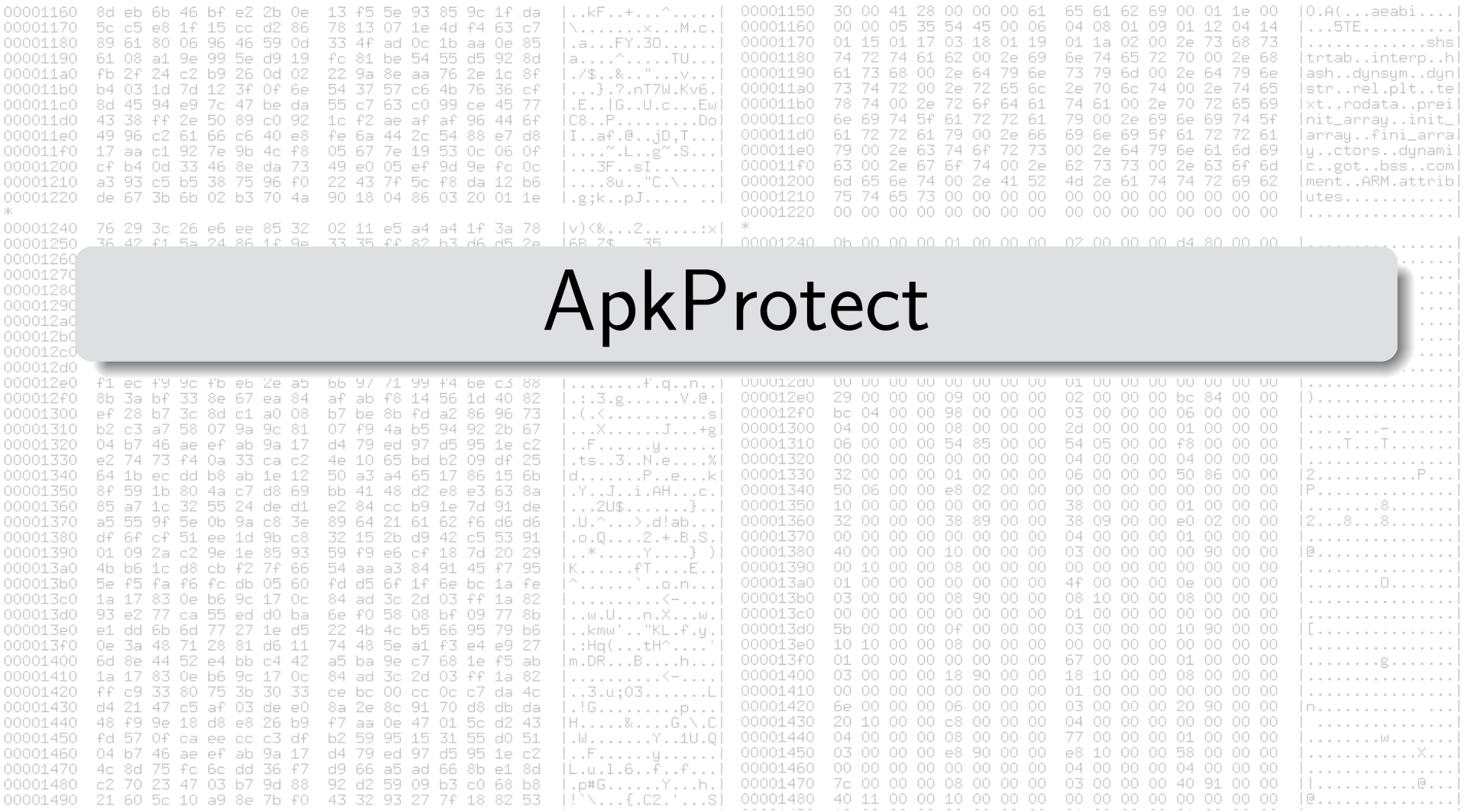
HoseDex2Jar

How does it work?

- 0x70 byte Dex header size not enforced
- Original Dex encrypted
- Added at the end of Dex header

Unpacker

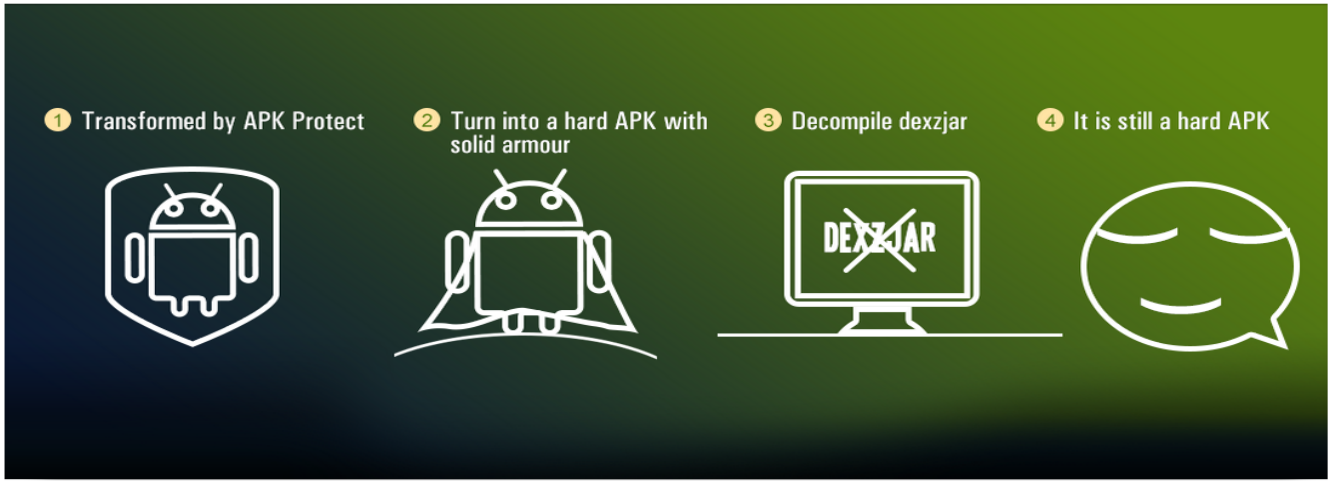
`https://github.com/strazzere/dehoser`



ApkProtect

ApkProtect

apkprotect.com



ApkProtect

Obfuscation in Dex

- Base64 encoding
- Java Reflection
- DES

ApkProtect

Obfuscation in Dex

- Base64 encoding
- Java Reflection
- DES

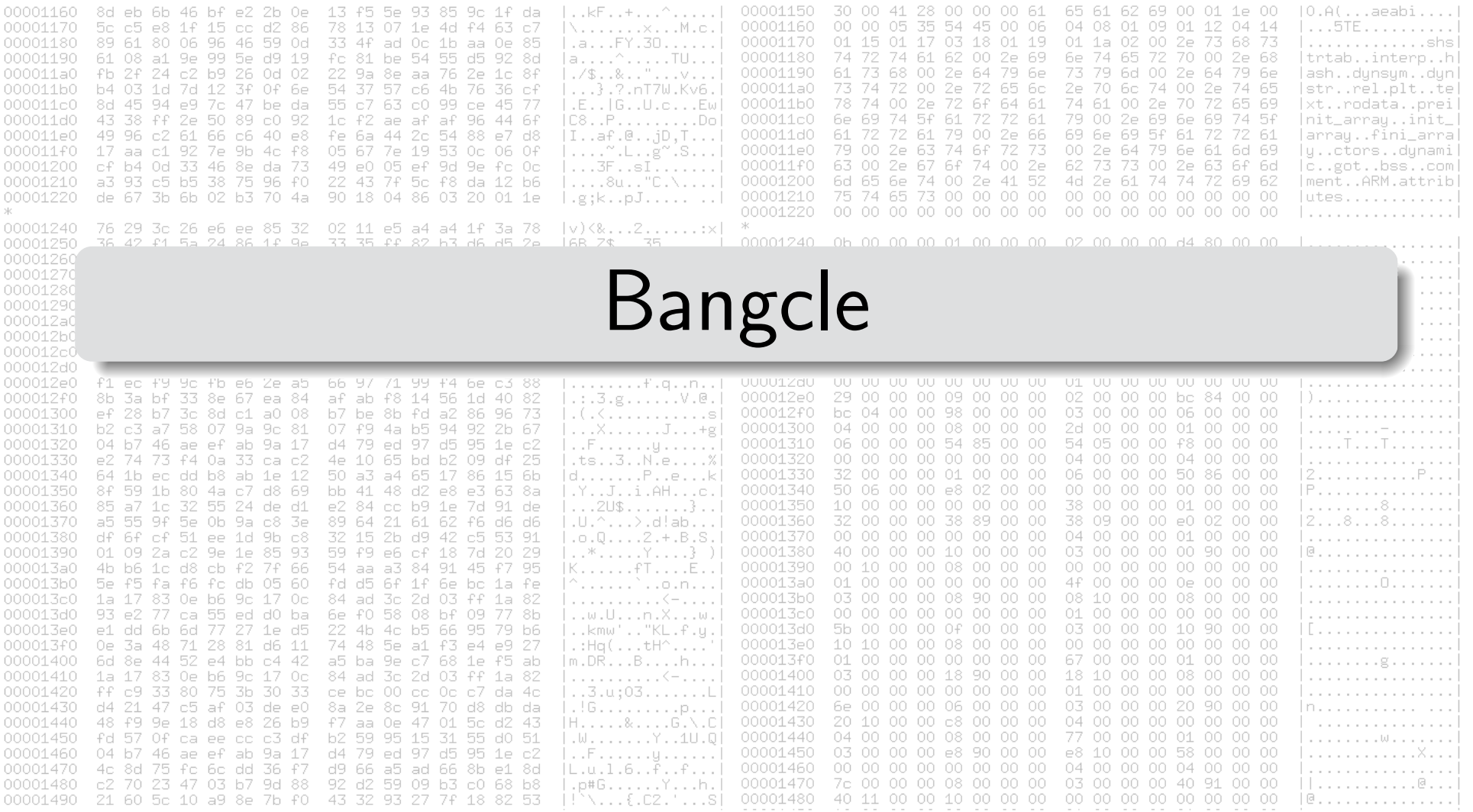
Details :

How Android Malware Fights (and we fight back!)
- CARO, May 2014

Props to

- @cryptax
- Andrubis Analysis Report reveals key

Bangcle



Bangcle

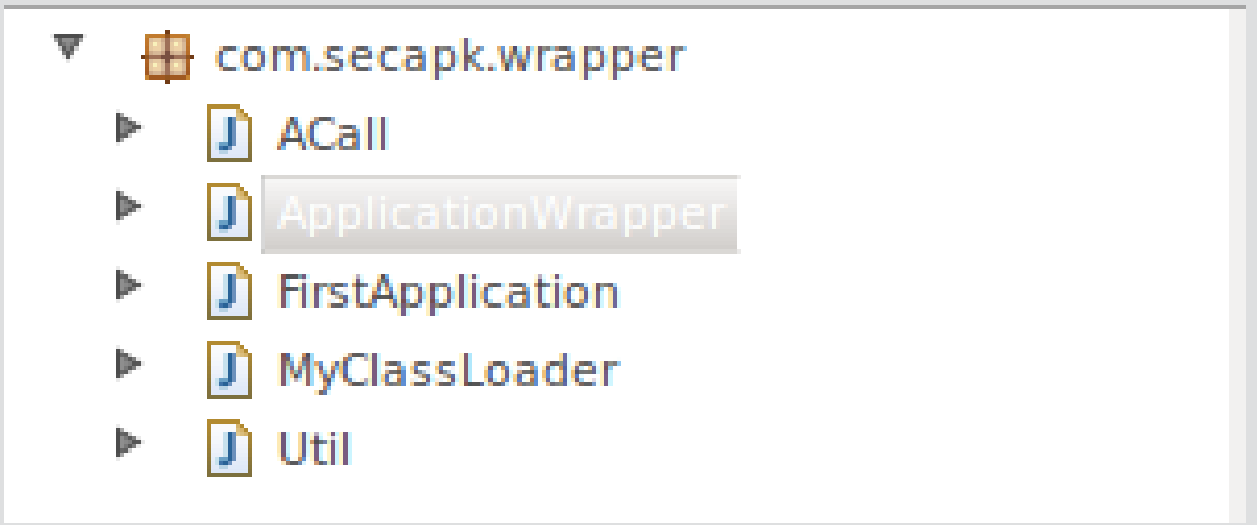
How does it work?

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

Bangcle - Static Analysis

Resistance to Static Analysis

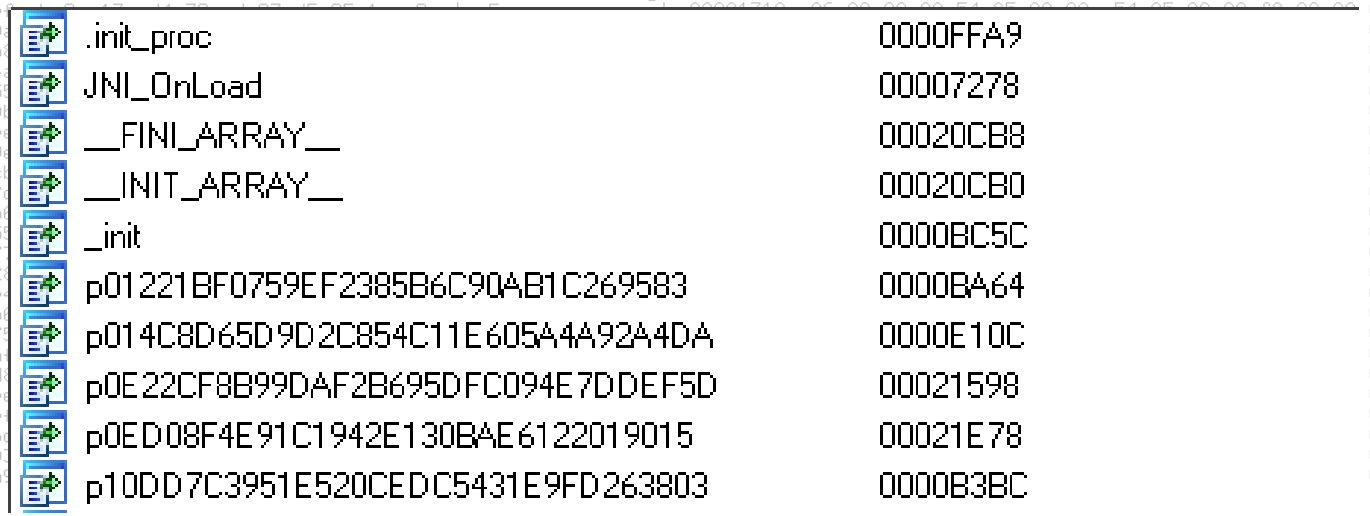
- Main Activity?



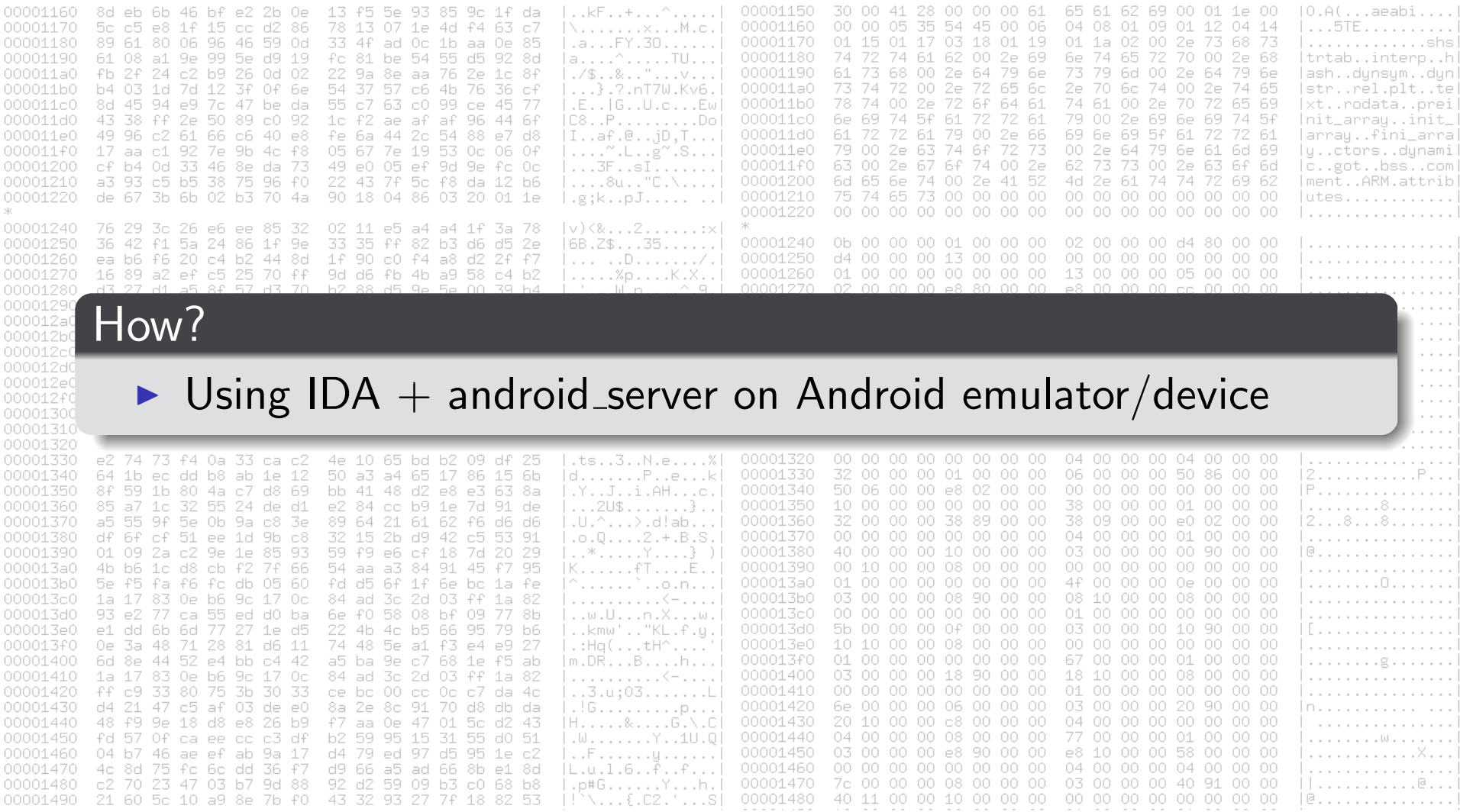
Bangcle - Static Analysis

Resistance to Static Analysis

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



Bangcle - Dynamic Analysis



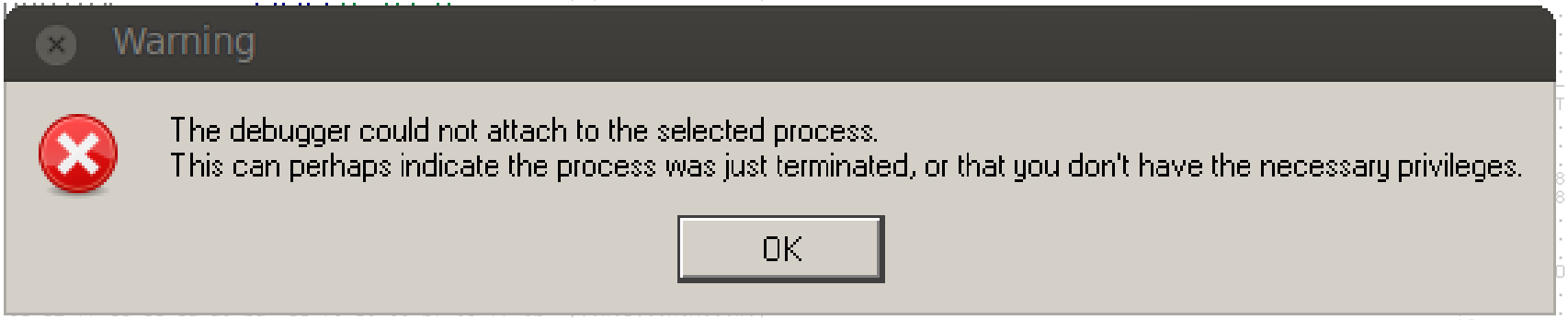
How?

- Using IDA + android_server on Android emulator/device

Bangcle - Dynamic Analysis

Anti-Debugging Tricks

- IDA can't attach to main process



Bangcle - Dynamic Analysis

Anti-Debugging Tricks

- IDA can't attach to main process
- Can't strace

```
root@android:/ # strace -p 10158
attach: ptrace(PTRACE_ATTACH, ...): Operation not permitted
```

Bangcle - Dynamic Analysis

Anti-Debugging Tricks

Attach to child process

- Hooked Standard libc Functions

```
libc.so:40036E78
libc.so:40036E78 __mmap2                        ; CODE XREF: libc.so:mmap+26↓p
libc.so:40036E78 LDR    PC, =(pAC6A2FD3BA9DCAFEE69830759164A81E+1)
libc.so:40036E78 ; End of function __mmap2
libc.so:40036E78
libc.so:40036E78 ; ---------------------------------------------------------------
```

- __open, read, write, close, munmap, msync
- Can't stack backtrace

Bangcle - Dynamic Analysis

Only in Memory

```
LOAD:000070BC ; ---------------------------------------------------------------
LOAD:000070BC
LOAD:000070BC                 EXPORT so_main
LOAD:000070BC so_main
LOAD:000070BC                 LDMIA   R6, {R0,R3,R6,R7}
LOAD:000070BE                 STR     R2, [R2,#0x48]
LOAD:000070C0                 STR     R2, [R7,R2]
LOAD:000070C2                 LDRB    R0, [R3,R6]
LOAD:000070C4                 SUBS    R0, R5, #6
LOAD:000070C6                 MOVS    R1, #0x92 ; 'Æ'
LOAD:000070C6 ; ---------------------------------------------------------------
LOAD:000070C8                 DCD 0x5E13FB25, 0x4878EF4A, 0x3C8AFD6C, 0xD76D243F
LOAD:000070D8 ; ---------------------------------------------------------------
LOAD:000070D8
LOAD:000070D8 loc_70D8                ; CODE XREF: LOAD:000071B8↓j
LOAD:000070D8                 ADDS    R6, #0x7A ; 'z'
LOAD:000070DA                 ASRS    R2, R0, #5
LOAD:000070DC                 BGE     loc_71D2
LOAD:000070DE                 BGE     loc_7182
LOAD:000070E0                 CMP     R3, #0x22 ; '"'
LOAD:000070E2                 SUBS    R3, R6, #2
LOAD:000070E4                 LDR     R6, =0x5D7BA519
LOAD:000070E6                 BEQ     loc_71C8
LOAD:000070E8                 SBCS    R6, R7
LOAD:000070EA                 ADDS    R2, R4, #4
LOAD:000070EC                 ADD     R2, SP, #0x204
LOAD:000070EE                 B       loc_6954
LOAD:000070EE ; ---------------------------------------------------------------
LOAD:000070F0                 DCD 0xFEA59D7A, 0xDDECAF8D, 0x4F6D99B9, 0xC19C7DB6, 0xBC49FB1C
LOAD:000070F0                 DCD 0xADD01C39, 0x410BA8EB, 0x721D281, 0x92656034, 0x4A587743
LOAD:00007118 ; ---------------------------------------------------------------
LOAD:00007118                 CBZ     R0, loc_7196
LOAD:00007118
LOAD:0000711A
LOAD:0000711A loc_711A                ; CODE XREF: LOAD:000071D4↓j
LOAD:0000711A                 B       loc_72B6
LOAD:0000711A ; ---------------------------------------------------------------
LOAD:0000711C                 DCB 0xA0 ; á
```

```
LOAD:4009F0BC ; =============== S U B R O U T I N E =======================================
LOAD:4009F0BC
LOAD:4009F0BC
LOAD:4009F0BC EXPORT so_main
LOAD:4009F0BC so_main
LOAD:4009F0BC
LOAD:4009F0BC var_60= -0x60
LOAD:4009F0BC var_54= -0x54
LOAD:4009F0BC
LOAD:4009F0BC PUSH   {R4-R7,LR}
LOAD:4009F0BE MOV    R7, R11
LOAD:4009F0C0 MOV    R6, R10
LOAD:4009F0C2 MOV    R5, R9
LOAD:4009F0C4 MOV    R4, R8
LOAD:4009F0C6 PUSH   {R4-R7}
LOAD:4009F0C8 LDR    R4, =(_GLOBAL_OFFSET_TABLE_ - 0x4009F0D2)
LOAD:4009F0CA SUB    SP, SP, #0x3C
LOAD:4009F0CC LDR    R2, =(alzocaz1qgymxed - 0x4009F0DA)
LOAD:4009F0CE ADD    R4, PC ; _GLOBAL_OFFSET_TABLE_
LOAD:4009F0D0 STR    R4, [SP,#0x60+var_60]
LOAD:4009F0D2 LDR    R4, =(aAssetsMetaData - 0x4009F0DC)
LOAD:4009F0D4 STR    R1, [SP,#0x60+var_54]
LOAD:4009F0D6 ADD    R2, PC ; alzocaz1qgymxed      ; "iZOCAZ1qGYMXEdPWGNq3S5SjikOW77=="
LOAD:4009F0D8 ADD    R4, PC                        ; "assets/meta-data/manifest.mf"
LOAD:4009F0DA ADDS   R4, #0x60 ; '`'
LOAD:4009F0DC MOVS   R3, R4
LOAD:4009F0DE LDMIA  R2!, {R0,R5,R7}               ; "iZOCAZ1qGYMXEdPWGNq3S5SjikOW77=="
LOAD:4009F0E0 STMIA  R3!, {R0,R5,R7}
LOAD:4009F0E2 LDMIA  R2!, {R1,R5,R7}
LOAD:4009F0E4 STMIA  R3!, {R1,R5,R7}
LOAD:4009F0E6 LDMIA  R2!, {R0,R1}
LOAD:4009F0E8 STMIA  R3!, {R0,R1}
LOAD:4009F0EA LDR    R1, =(a7fwqmsn5ptciuo - 0x4009F0F4)
LOAD:4009F0EC LDRB   R2, [R2]
LOAD:4009F0EE MOVS   R0, R4
LOAD:4009F0F0 ADD    R1, PC ; a7fwqmsn5ptciuo      ; "7FwQmsN5PtciUOpfL1Y/erd4zSEGAbg9I+328qv"...
LOAD:4009F0F2 STRB   R2, [R3]
LOAD:4009F0F4 BL     sub_4009E350
```

Figure : Decrypted library in memory

Bangcle

Security Enforcements by bangcle.com

- Applications are scanned before packing
- **LIMITATION:** Fails to detect new/unknown malware.

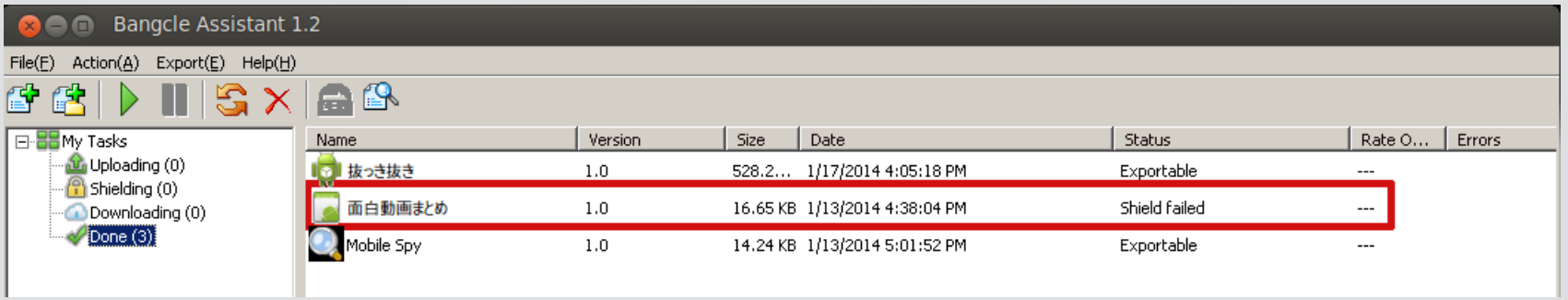
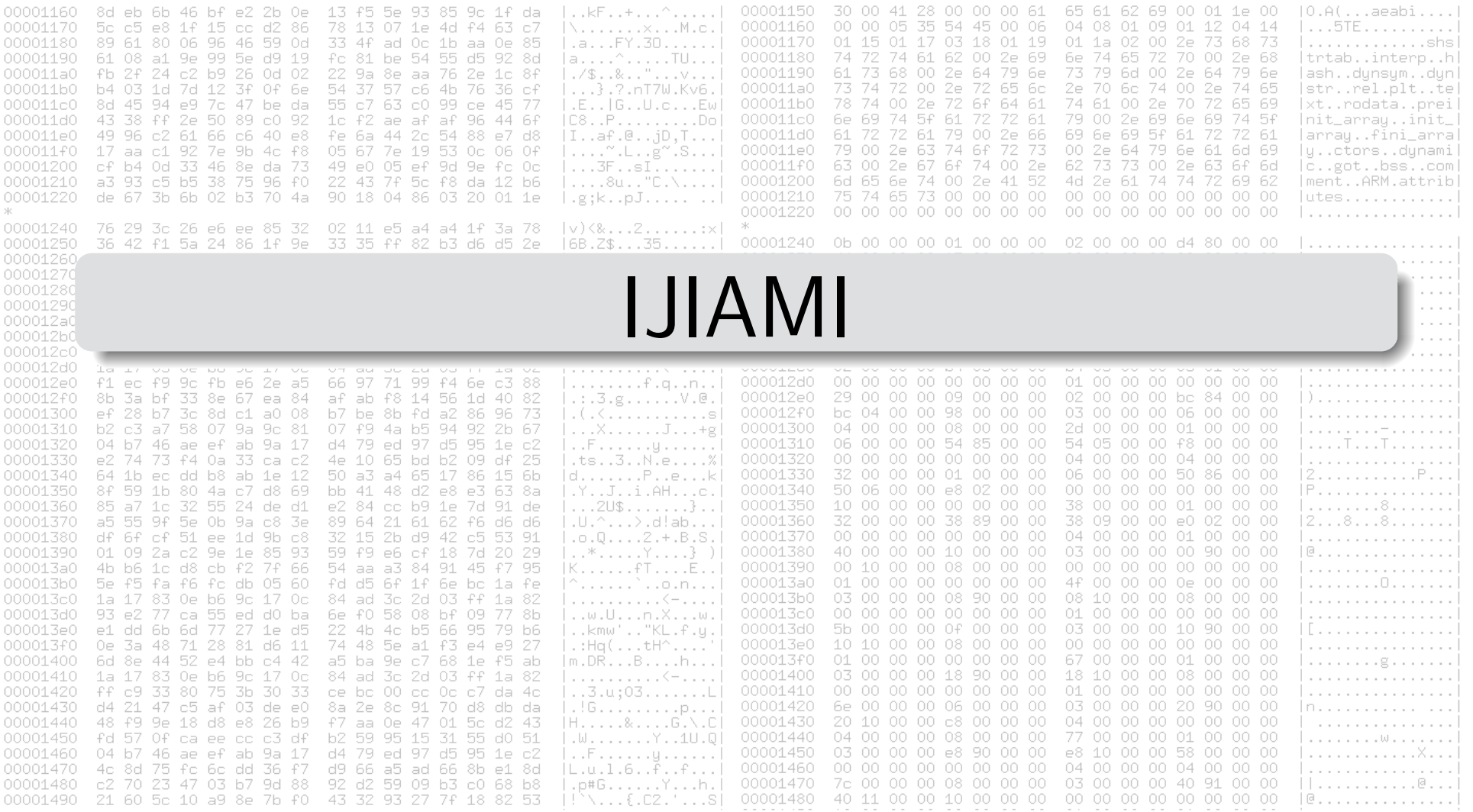


Figure : Rejected Application : Shield Failed

IJIAMI



Ijiami

Dynamically linked shared libraries

Security Enforcements by ijiami.cn

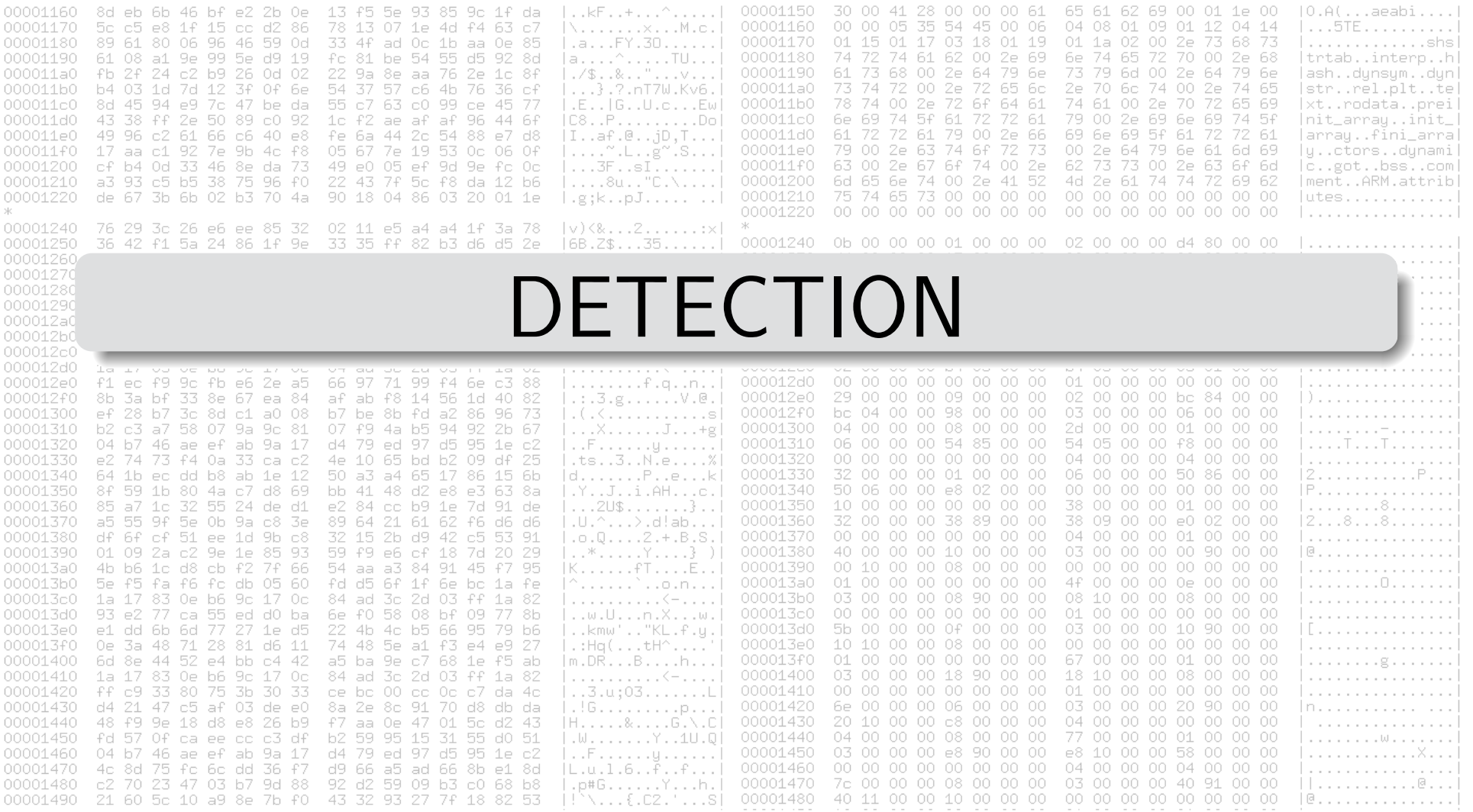
- Accounts reviewed at the time of creation
- Uploaded applications 'audited' before packing
- **HIGHER SECURITY?** Rejected app that passed Bangcle's security test

Packed malware in the wild

Known samples

- HoseDex2Jar - No known malware
- ApkProtect - Android/SmsSend.ND!tr SMS sending malware
- Bangcle packed malware
  - Android/Feejar.B!tr
  - Android/FakeIns.D
  - Adware/Waps!Android etc

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
00001270
00001280
00001290
000012a0
000012b0
000012c0
000012d0
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 |................|
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 00 90 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 |@...............|

Detection

Visible Signs? Eg: Bangcle

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

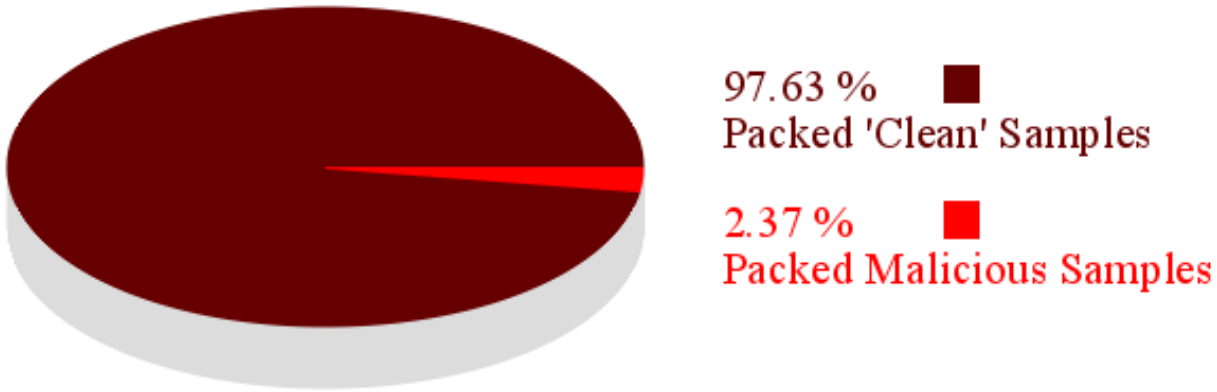
Detection

Visible Signs? Eg: Bangcle

Drawback

FALSE POSITIVES!

FP Rate = 97.63%



Detection

Solution

- Every new packer in market = ¿ Write new unpacker
  OR
- Run every sample on emulator or VM

Challenges for Automation

- Must unpack before signing
- Time + Resource tradeoff between static & dynamic detection

The End

Thank you for listening!

Contact

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