



Separating from the pack

FortiGuard Labs,
FORTINET

11th October, 2014

FortiGuard Labs
Threat Research and Response



Today's Agenda



```
00001160 8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da |.kF.+...^....| 00001150 30 00 41 28 00 00 00 61 65 61 62 69 00 01 1e 00 |0.A[...aebi....|
00001170 5c c5 e8 1f 15 c0 d2 8e 78 13 07 1e 4d f4 63 c7 |\\.....x...M.c.| 00001160 00 00 05 35 54 45 00 06 04 08 01 09 01 12 04 14 |...5TE.....|
00001180 89 61 80 06 96 46 59 d0 33 4f ad 0c 1b aa 0e 85 |.S...FY.3D....| 00001170 01 15 01 17 03 18 01 19 01 1a 02 00 2e 73 68 73 |.....shs|
00001190 61 09 a1 9e 99 5e d9 19 fc 81 be 54 55 d5 92 8d |a.....TU....| 00001180 74 72 74 61 62 00 2e 69 6e 74 65 72 70 00 2e 68 |trtab..interp.h|
000011a0 fb 2f 24 c2 b9 26 d0 02 22 9a 8e aa 76 2e 1c 8f |.$.&...".v....| 00001190 61 73 68 00 2e 64 79 6e 73 79 6d 00 2e 64 79 6e |ash..dynsym..dyn|
000011b0 b4 03 1d 7d 12 3f 0f 6e 54 37 57 c6 4b 76 36 cf |...}.?..nT7M.Kv6.| 000011a0 73 74 72 00 2e 72 65 6c 2e 70 6c 74 00 2e 74 65 |str..rel.plt..te|
000011c0 8d 45 94 e9 7c 47 be da 55 c7 63 c0 99 ce 45 77 |.E..|G..U.c...Ew| 000011b0 78 74 00 2e 72 6f 64 61 74 61 00 2e 70 72 65 69 |xt..rodata..prei|
000011d0 43 38 ff 2e 50 89 c0 92 1c f2 ae af af 96 44 6f |C8..P.....Do| 000011c0 6e 69 74 5f 61 72 72 61 79 00 2e 69 6e 69 74 5f |init_array..init_|
000011e0 49 96 c2 61 66 c6 40 e8 fe 6a 74 2c 54 88 e7 d8 |I..af..@..j0,T..| 000011d0 61 72 72 61 79 00 2e 66 69 6e 69 5f 61 72 72 61 |array..fini_arra|
000011f0 17 aa c1 92 7e 9b 4c f8 05 67 7e 19 53 0c 06 0f |...".L.g".S....| 000011e0 79 00 2e 63 74 6f 72 73 00 2e 64 79 6e 61 6d 69 |y..ctors..dynam|
00001200 cf b4 d0 33 46 8e da 73 49 e0 05 ef 9d 9e fc 0c |...3F..eI.....| 000011f0 63 00 2e 67 6f 74 00 2e 62 73 73 00 2e 63 6f 6d |c..got..bse...com|
00001210 *|.....trib|
00001220 |.....|
00001230 |.....|
00001240 |.....|
00001250 |.....|
00001260 |.....|
00001270 |.....|
00001280 |.....|
00001290 |.....|
00001300 |.....|
00001310 |.....|
00001320 |.....|
00001330 |.....|
00001340 |.....|
00001350 |.....|
00001360 |.....|
00001370 |.....|
00001380 |.....|
00001390 |.....|
00001400 6d 8e 44 52 e4 bb c4 42 a5 ba 9e c7 68 1e f5 ab |m.DR...B...h...| 000013f0 01 00 00 00 00 00 00 00 67 00 00 00 01 00 00 00 |.....g.....|
00001410 1a 17 83 0e b6 9c 17 0c 84 ad 3c 2d 03 ff 1a 82 |.....<.....| 00001400 03 00 00 00 18 90 00 00 18 10 00 00 08 00 00 00 |.....|
00001420 ff c9 33 80 75 3b 30 33 ce bc 00 cc 0c c7 da 4c |...3..u03.....L| 00001410 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 |.....|
00001430 d4 21 47 c5 af 03 de e0 8a 2e 8c 91 70 d8 db da |.G.....p....| 00001420 6e 00 00 00 06 00 00 00 03 00 00 00 20 90 00 00 |n.....|
00001440 48 f9 9e 18 d8 e8 26 b9 f7 aa 0e 47 01 5c d2 43 |H.....&...G..C| 00001430 20 10 00 00 c8 00 00 00 04 00 00 00 00 00 00 00 |.....|
00001450 fd 5f 0f ca ee cc c3 df b2 59 95 15 31 55 d0 51 |.M.....Y...1U.Q| 00001440 04 00 00 08 08 00 00 00 77 00 00 00 01 00 00 00 |.....|
00001460 04 b7 46 ae ef ab 9a 17 d4 79 ed 97 d5 95 1e c2 |.F.....Y.....| 00001450 03 00 00 00 e8 90 00 00 e8 10 00 00 58 00 00 00 |.....|
00001470 4c 8d 75 fc 6c dd 36 47 d9 66 a5 ad 66 8b e1 8d |.L..l.G..F..F..| 00001460 00 00 00 00 00 00 00 00 04 00 00 00 04 00 00 00 |.....|
00001480 c2 70 23 47 03 bf 9d 88 92 d2 59 09 b3 c0 68 b8 |.p#G.....Y...h| 00001470 7c 00 00 00 08 00 00 00 03 00 00 00 04 91 00 00 |.....|
00001490 21 60 5c 10 a9 8e 7b f0 43 32 93 27 7f 18 82 83 |!\\...{.C2....S| 00001480 40 11 00 00 10 00 00 00 00 00 00 00 00 00 00 00 |B.....|
```

- ▶ 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

What are Packers

- Mainly just compression eg: ZIP, RAR



```

00001160 8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da |...k.f.,+...^....| 00001150 30 00 41 28 00 00 00 61 65 61 62 69 00 01 1e 00 |0.A[...aeabi....|
00001170 5c c5 e8 1f 15 c0 d2 86 78 13 07 1e 4d f4 63 c7 |...x...M.c...| 00001160 00 00 05 35 54 45 00 06 04 08 01 09 01 12 04 14 |...5TE.....|
00001180 89 61 80 06 96 46 59 0d 33 4f ad 0c 1b aa 0e 85 |...PY.3D....| 00001170 01 15 01 17 03 18 01 19 01 1a 02 00 2e 73 68 73 |...shs.....|
00001190 61 08 a1 9e 99 5e 49 19 f3 81 be 54 55 05 92 8d |...TU....| 00001180 74 72 74 61 62 00 2e 69 6e 74 65 72 70 00 2e 68 |t.rtab.interp.h
000011a0 fb 2f 24 c2 b9 26 0d 02 22 9a 8e aa c6 2e 1c 8f |...$.k...v...| 00001190 61 73 68 00 2e 64 79 6e 73 79 6d 00 2e 64 79 6e |ash..dynsym..dyn
000011b0 b4 03 1d 7d 18 3f 0f 6e 54 37 57 c6 4b 76 36 cf |...?.nT7M.Kv6..| 000011a0 73 74 72 00 2e 72 65 6c 2e 70 6c 74 00 2e 74 65 |str..rel.plt..te
000011c0 8d 45 94 e9 7c 47 be da 55 c7 63 c0 99 ce 45 77 |...G..U.c...Ew| 000011b0 78 74 00 2e 72 6f 64 61 74 61 00 2e 70 72 65 69 |xt..rodata..prei
000011d0 43 38 ff 2e 50 c0 92 1c f2 ae af 96 44 6f 6f |...J..nT7M.Kv6..| 000011c0 6e 69 74 5f 61 72 72 61 79 00 2e 69 6e 69 74 5f |nit.array..init_
000011e0 49 96 c2 61 66 c6 40 e8 fe 6a 44 2c 54 88 e7 d8 |...af..B..J..T...| 000011d0 61 72 72 61 79 00 2e 66 69 6e 69 5f 61 72 72 61 |array..fini arra
000011f0 17 aa c1 92 7e 9b 4c f8 05 67 7e 19 53 0c 06 0f |...L..B...S...| 000011e0 79 00 2e 63 74 6f 72 73 00 2e 64 79 6e 61 6d 69 |y..ctors..dynam
00001200 cf b4 0d c3 46 8e da 73 49 e0 05 ef 9d 9e fc 0c |...F..f..l...| 000011f0 63 00 2e 67 6f 74 00 2e 62 73 73 00 2e 63 6f 6d |c..got..bss..com
00001210 a3 93 c5 b5 75 96 40 22 43 7f 5c f8 da 12 b6 |...8u...C...| 00001200 6d 65 6e 74 00 2e 41 52 4d 2e 61 74 74 72 69 62 |ment..ARM.attrib
00001220 de 67 3b 6b 02 b3 70 4a 90 18 04 66 03 20 01 1e |...g.k..pJ....| 00001210 75 74 65 73 00 00 00 00 00 00 00 00 00 00 00 |utes.....|
*
00001230
00001240
00001250
00001260
00001270
00001280
00001290
00001300
00001310
00001320
00001330
00001340
00001350
00001360
00001370
00001380
00001390
00001400
00001410
00001420
00001430
00001440
00001450
00001460
00001470
00001480
00001490

```

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

```

000013b0 9e f3 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 |...0123456789ABCDEF| 000013a0 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 |0123456789ABCDEF|
000013c0 1a 17 83 0e b6 9c 17 0c 84 ad 3c 2d 03 ff 1a 82 |...<.....| 000013b0 03 00 00 00 08 90 00 00 08 10 00 00 08 00 00 00 |0810000008000000|
000013d0 93 e2 77 ca 55 ed 0d ba 6e f0 58 08 bf 09 77 8b |...U...n.X..w...| 000013c0 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 |0100000000000000|
000013e0 e1 dd 6b 6d 77 27 1e d5 22 4b 4c b5 65 95 79 b6 |...k.m...*KL.F.y..| 000013d0 5b 00 00 00 0f 00 00 00 03 00 00 00 10 90 00 00 |[.....].....|
000013f0 0e 3a 48 71 28 e1 d6 11 74 48 5e a1 f3 e4 e9 27 |...Hq[...tH.....| 000013e0 10 10 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 |101000000f000000|
00001400 6d 8e 44 52 e4 bb c4 12 a5 ba 9e c7 68 1e f5 ab |m.DR...B...h...| 000013f0 01 00 00 00 00 00 00 00 67 00 00 00 01 00 00 00 |...g.....|
00001410 1a 17 83 0e b6 9c 17 0c 84 ad 3c 2d 03 ff 1a 82 |...<.....| 00001400 03 00 00 00 18 90 00 00 18 10 00 00 08 00 00 00 |1810000008000000|
00001420 ff c9 33 30 75 3b 30 33 ce bc 00 cc 0c c7 da 4c |...3..u03...L...| 00001410 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 |0100000000000000|
00001430 d4 21 47 c5 af 0f 0d 8a 2e 8c 91 70 d8 db da |...G.....p...| 00001420 6e 00 00 00 06 00 00 00 03 00 00 00 20 90 00 00 |n.....|
00001440 48 f9 9e 18 d8 e8 26 b9 f7 aa 9e 47 01 5c d2 43 |H.....&...G..C| 00001430 20 10 00 00 c8 00 00 00 04 00 00 00 00 00 00 00 |0400000000000000|
00001450 fd 5f 0f ca ee cc c3 df 62 59 95 13 55 0d 51 |...M.....Y..1U.Q| 00001440 04 00 00 08 08 00 00 00 77 00 00 00 01 00 00 00 |...M.....|
00001460 04 b7 46 ae ef ab 9a 17 d4 79 ed 97 d5 95 1e c2 |...F.....| 00001450 03 00 00 00 e8 90 00 00 e8 10 00 00 58 00 00 00 |...F.....|
00001470 4c 8d 75 fc 6c dd 36 47 09 66 a5 ad 66 8b e1 8d |...u..1.G..F..f..| 00001460 00 00 00 00 00 00 00 00 04 00 00 00 04 00 00 00 |...B.....|
00001480 c2 70 23 47 03 bf 9d 88 92 d2 59 09 b3 c0 68 b8 |...pG.....Y...h..| 00001470 7c 00 00 08 00 00 00 00 03 00 00 00 40 91 00 00 |...B.....|
00001490 21 60 5c 10 a9 8e 7b 0f 43 32 93 27 7f 18 82 83 |...C2....S...| 00001480 40 11 00 00 10 00 00 00 00 00 00 00 00 00 00 00 |B.....|

```

```
00001160 8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da |..kF...+...^....| 00001150 30 00 41 28 00 00 00 61 65 61 62 69 00 01 1e 00 |0.A[...aebi....|
00001170 5c c5 e8 1f 15 c0 d2 86 78 13 07 1e 4d f4 63 c7 |\.....x...M.c..| 00001160 00 00 05 35 54 45 00 06 04 08 01 09 01 12 04 14 |...5TE.....|
00001180 89 61 80 06 96 46 59 d0 33 4f ad 0c 1b aa 0e 85 |.a...FY.3D.....| 00001170 01 15 01 17 03 18 01 19 01 1a 02 00 2e 73 68 73 |...shs|
00001190 61 08 a1 9e 99 5e d9 19 fc 81 be 54 55 d5 92 8d |a.....TU.....| 00001180 74 72 74 61 62 00 2e 69 6e 74 65 72 70 00 2e 68 |trtab..interp..h|
000011a0 fb 2f 24 c2 99 26 d0 02 22 9a 8e aa 76 2e 1c 8f |.$.&...v.....| 00001190 61 73 68 00 2e 64 79 6e 73 79 6d 00 2e 64 79 6e |ash..dynsym..dyn|
000011b0 b4 03 1d 7d 12 3f 0f 6e 54 37 57 c6 4b 76 36 cf |.j..?..nT7M.Kv6..| 000011a0 73 74 72 00 2e 72 65 6c 2e 70 6c 74 00 2e 74 65 |str..rel.plt..te|
000011c0 4d 45 94 e9 7c 47 8b da 55 c7 63 c0 99 ce 45 77 |.E..[G..U.c...Ew| 000011b0 78 74 00 2e 72 6f 64 61 74 61 00 2e 70 72 65 69 |xt..rodata..prei|
000011d0 83 38 ff 2e 50 c9 c0 92 1c f2 ae af 96 44 6f |C8..P.....Do| 000011c0 6e 69 74 5f 61 72 72 61 79 00 2e 69 6e 69 74 5f |nit.array..init_|
000011e0 49 96 c2 61 66 c6 40 e8 fe 6a 44 2c 54 88 e7 d8 |I..af..B...Q.T..| 000011d0 61 72 72 61 79 00 2e 66 69 6e 69 5f 61 72 72 61 |array..fini_arra|
000011f0 17 aa c1 92 7e 9b 4c f8 05 67 7e 19 53 0c 06 0f |...L..g...S.....| 000011e0 79 00 2e 63 74 6f 72 73 00 2e 64 79 6e 61 6d 69 |y..ctors..dynam|
00001200 cf b4 0d c3 46 8e da 73 49 e0 05 ef 9d 9e fc 0c |...3F...l.....| 000011f0 63 00 2e 67 6f 74 00 2e 62 73 73 00 2e 63 6f 6d |c..got..bss..com|
00001210 a3 93 c5 b5 38 75 96 f0 22 43 7f 5c f9 da 12 b6 |...8u...C.....| 00001200 6d 65 6e 74 00 2e 41 52 4d 2e 61 74 72 69 62 |ment..ARM.attrib|
00001220 *
00001230
00001240
00001250
00001260
00001270
00001280
00001290
00001300
00001310
00001320
00001330
00001340
00001350
00001360
00001370
00001380
00001390
00001400
00001410
00001420
00001430
00001440
00001450
00001460
00001470
00001480
00001490
00001300 e1 dd 6b 6d 77 27 1e d5 22 4b 4c b5 66 95 79 b6 |..kmm'...TKL.F-y..| 000013d0 5b 00 00 00 0f 00 00 00 03 00 00 00 10 90 00 00 |[.....|
000013f0 0e 3a 48 71 28 81 d6 11 74 48 5e a1 f3 e4 e9 27 |..Hq(...tH"...| 000013e0 10 10 00 00 08 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001400 6d 8e 44 52 e4 bb c4 42 a5 ba 9e c7 68 1e f5 ab |m.DR...B...h...| 000013f0 01 00 00 00 00 00 00 00 67 00 00 00 01 00 00 00 |.....g.....|
00001410 1a 17 83 0e b6 9c 17 0c 84 ad 3c 2d 03 ff 1a 82 |...3..u;03...L..| 00001400 03 00 00 00 18 90 00 00 18 10 00 00 08 00 00 00 |.....|
00001420 ff c9 33 80 75 3b 30 33 ce bc 00 cc 0c c7 da 4c |.G...P.....p...| 00001410 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 |.....|
00001430 d4 21 47 c5 af 03 de e0 8a 2e 8c 91 70 d8 db da |H.....&...G..C| 00001420 6e 00 00 00 06 00 00 00 03 00 00 00 20 90 00 00 |n.....|
00001440 48 f9 9e 18 d8 e8 26 b9 f7 aa 0e 47 01 5c d2 43 |.W.....Y...1U.Q| 00001430 20 10 00 00 c8 00 00 00 04 00 00 00 00 00 00 00 |.....|
00001450 fd 57 0f ca ee cc c3 df b2 59 95 15 31 55 d0 51 |..F.....Y...| 00001440 04 00 00 08 08 00 00 00 77 00 00 00 01 00 00 00 |.....|
00001460 04 b7 46 ae ef ab 9a 17 d4 79 ed 97 d5 95 1e c2 |.F.....Y...| 00001450 03 00 00 00 e8 90 00 00 e8 10 00 00 58 00 00 00 |.....|
00001470 4c 8d 75 fc 6c dd 36 47 d9 66 a5 ad 66 8b e1 8d |.u..1.G...Y...F..| 00001460 00 00 00 00 00 00 00 00 04 00 00 00 04 00 00 00 |.....|
00001480 c2 70 23 47 03 bf 9d 88 92 d2 59 09 b3 c0 68 b8 |.pG.....Y...h..| 00001470 7c 00 00 00 08 00 00 00 03 00 00 00 91 00 00 00 |.....|
00001490 21 60 5c 10 a9 8e 7b f0 43 32 93 27 7f 18 82 83 |!\...\{C2...sS..| 00001480 40 11 00 00 10 00 00 00 00 00 00 00 00 00 00 00 |B.....|
```

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



00001160	8d eb 6b 46 bf e2 2b 0e	13 f5 5e 93 85 9c 1f da	..k.f.+.+.+.+.+.+.+	00001150	30 00 41 28 00 00 00 61	65 61 62 69 00 01 1e 00	0.A[...aeebi....	
00001170	5c e5 e8 1f 15 c0 d2 86	78 13 07 1e 4d f4 63 c7	..x...x...M.c..	00001160	00 00 05 35 54 45 00 06	04 08 01 09 01 12 04 14	...5TE.....	
00001180	89 61 80 06 96 46 59 d0	33 4f ad 0c 1b aa 0e 85	..b...fY.30.....	00001170	01 15 01 17 03 18 01 19	01 1a 02 00 2e 73 68 73	...shs	
00001190	61 08 a1 9e 99 5e d9 19	7c 81 be 54 05 92 8d 6f	a.....TU.....	00001180	74 72 74 61 62 00 2e 69	6e 74 65 72 70 2e 2e 68	..t..tab..interp..h	
000011a0	fb 2f 24 c2 b9 26 d0 02	22 9a 8e aa 76 2e 1c 8f	./\$.&.....	00001190	61 73 68 00 2e 64 79 6e	73 79 6d 00 2e 64 79 6e	..ash..dynsym..dyn	
000011b0	b4 03 1d 7d 12 3f 0f 6e	54 37 57 c6 46 76 3e cf	..j..?..nTm.Kv6..	000011a0	73 74 72 00 2e 72 65 6c	2e 70 6c 74 00 2e 74 65	..str..rel.plt..tel	
000011c0	8d 45 94 e9 7c 47 be da	55 c7 63 c0 99 ce 45 77	..e..lG..U.c...Ew	000011b0	78 74 00 2e 72 6f 64 61	74 61 00 2e 70 72 65 69	..xt..rodata..prei	
000011d0	43 38 ff 2e 50 89 c0 92	1c f2 ae af 96 44 6f	Cb..P.....Do	000011c0	6e 69 74 5f 61 72 72 61	79 00 2e 69 6e 69 74 5f	..init..array..init_	
000011e0	49 96 c2 61 66 c6 40 e8	7e 6a 44 2c 54 88 e7 d8	..l..af..e..jD..T..	000011d0	61 72 72 61 79 00 2e 66	69 6e 69 5f 61 72 72 61	..array..fini..arra	
000011f0	17 aa c1 92 7e 9b 4c f8	05 67 7b 19 53 c0 06 0f	L..g...S..	000011e0	79 00 2e 63 74 6f 72 73	00 2e 64 79 6e 61 6d 69	..ly..ctors..dynami	
00001200	cf b4 0d 33 46 8e da 73	49 e0 05 ef 9d 9e fc c0	..f..f..e.l.....	000011f0	63 00 2e 67 6f 74 00 2e	62 73 73 00 2e 63 6f 6d	..c..got..bss..com	
00001210	a3 93 c5 38 75 9e 40	22 43 74 5c f9 da 12 b6	8u...C..X..	00001200	6d 65 6e 74 00 2e 41 52	4d 2e 61 74 74 72 69 62	..ment..ARM.attrib	
00001220	de 67 3b 6b 02 b3 70 4a	90 18 04 66 03 20 01 e1	..g..k..p..j.....	00001210	75 74 65 73 00 00 00 00	00 00 00 00 00 00 00 00	..utes.....	
00001230	*			00001220	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00		
00001240	76 29 3c 26 e6 ee 85 32	02 11 e5 a4 a4 1f 3a 78	v)<.....2.....x	00001230	0b 00 00 00 01 00 00 00	02 00 00 00 d4 80 00 00		
00001250	36 42 f1 5a 24 86 1f 9e	33 35 ff 82 b3 d6 d5 2e	l68.Z\$.....35.....	00001240	da 00 00 00 43 00 00 00	00 00 00 00 00 00 00 00		
00001260	aa b6 65 e0 c4 b2 d4 4a	1f 90 c0 64 a8 d2 2f c7						
00001270								
00001280								
00001290								
00001300								
00001310								
00001320								
00001330								
00001340								
00001350								
00001360								
00001370								
00001380								
00001390								
00001400								
00001410								
00001420								
00001430								
00001440								
00001450								
00001460								
00001470								
00001480								
00001490								

Relevance in Android Security?

- Intended Use
 - Code hiding
 - Tampering proof

00001370	ad cc 9f de 0d 9a c8 be	09 b4 c1 b3 b2 fb db db	..U...f..diaa...l	00001360	3c 00 00 00 3e 09 00 00	3e 09 00 00 00 00 00 00	..z...o.....
00001380	df 6f cf 51 ee 1d 9b c8	32 15 2b 49 42 c5 53 91	..o.q.....2...B.S..	00001370	00 00 00 00 00 00 00 00	00 00 00 00 01 00 00 00	
00001390	01 09 2a 4e 1e 85 93	89 89 e6 cf 18 7d 20 29	..o.q.....2...B.S..	00001380	40 00 00 00 10 00 00 00	03 00 00 00 00 90 00 00	..@.....
000013a0	4b 1e 6c c8 f2 7f 56	89 89 e6 cf 18 7d 20 29	..o.q.....2...B.S..	00001390	00 10 00 00 08 00 00 00	00 00 00 00 00 00 00 00	
000013b0	5e 1f 78 f6 fc 0e 05 60	fd d5 6f 1f 6e bc 1a fe	..o.q.....2...B.S..	000013a0	01 00 00 00 00 00 00 00	4f 00 00 00 0e 00 00 00	
000013c0	1a 17 83 0e b6 9c 17 0c	84 ad 3c 2d 03 ff 1a 82	..o.q.....2...B.S..	000013b0	03 00 00 00 08 90 00 00	08 10 00 00 08 00 00 00	
000013d0	93 e2 77 6a 55 ed d0 ba	6e 0f 58 08 bf 09 77 8b	..o.q.....2...B.S..	000013c0	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00	
000013e0	e1 dd 6b 6d 77 27 1e d5	22 4b ac c4 b5 66 95 79 b6	..o.q.....2...B.S..	000013d0	5b 00 00 00 0f 00 00 00	03 00 00 00 10 90 00 00	..[.....
000013f0	0e 3a 48 71 28 61 d6 11	74 48 5e ad f3 e4 45 89 27	..o.q.....2...B.S..	000013e0	10 10 00 00 08 00 00 00	00 00 00 00 00 00 00 00	
00001400	6d 8e 44 52 e4 bb c4 a2	45 ba 9e c7 68 1e f5 ab	..o.q.....2...B.S..	000013f0	01 00 00 00 00 00 00 00	67 00 00 00 01 00 00 00	
00001410	1a 17 83 0e b6 9c 17 0c	84 ad 3c 2d 03 ff 1a 82	..o.q.....2...B.S..	00001400	03 00 00 00 18 90 00 00	18 10 00 00 08 00 00 00	
00001420	ff c9 80 75 7b 3b 30 33	ce bc c0 00 c0 c0 c4 4c	..o.q.....2...B.S..	00001410	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00	
00001430	d4 21 47 c5 af d3 e0 8a	2e 8c 91 70 d8 db da	..o.q.....2...B.S..	00001420	5e 00 00 00 06 00 00 00	03 00 00 00 20 90 00 00	..n.....
00001440	48 f9 9e 18 08 e8 26 b9	f7 aa 0e 47 01 55 d2 43	..o.q.....2...B.S..	00001430	20 10 00 00 c8 00 00 00	04 00 00 00 00 00 00 00	
00001450	fd 57 0f ca ee cc c3 df	b2 59 95 19 31 55 80 81	..o.q.....2...B.S..	00001440	04 00 00 00 08 00 00 00	77 00 00 00 01 00 00 00	
00001460	04 b7 46 ae ef ab aa 17	d4 78 ed 97 d5 1e c2	..o.q.....2...B.S..	00001450	03 00 00 00 e8 90 00 00	e8 10 00 00 58 00 00 00	
00001470	4c 8d 75 fc 6c dd 3c 47	d9 66 a5 ad 66 b8 e1 8d	..o.q.....2...B.S..	00001460	00 00 00 00 00 00 00 00	04 00 00 00 04 00 00 00	
00001480	c2 70 23 47 03 9d 98	92 d2 59 09 2b c0 68 b8	..o.q.....2...B.S..	00001470	7c 00 00 00 08 00 00 00	03 00 00 00 40 91 00 00	
00001490	21 60 5c 10 a9 8e 7b 0f	43 32 93 27 7f 18 82 53	..o.q.....2...B.S..	00001480	40 11 00 00 10 00 00 00	00 00 00 00 00 00 00 00	..@.....

Relevance in Android Security?

- ▶ Intended Use
- ▶ Code hiding
- ▶ Tamperproofing



00001160	8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da	..kF...+...^....	00001150	30 00 41 28 00 00 00 61	65 61 62 69 00 01 1e 00	0.A[...aeabi....
00001170	5c c5 e8 1f 15 c0 d2 8e 78 13 07 1e 4d f4 63 c7	..S.....x...M.c.	00001160	00 00 05 35 54 45 00 06	04 08 01 09 01 12 04 14	...5TE.....shs
00001180	89 61 80 06 96 46 59 d0 33 4f ad 0c 1b aa 0e 85	..B...FY.3D....	00001170	01 15 01 17 03 18 01 19	01 1a 02 00 2e 73 68 73	..tstab.interp.h
00001190	61 08 a1 9e 99 5e d9 19 fc 81 be 54 55 d5 92 8d	a.....TU....	00001180	74 72 74 61 62 00 2e 69	6e 74 65 72 70 00 2e 68	..tash.dynsym.dyn
000011a0	fb 2f 24 c2 b9 26 0d 02 22 9a 8e aa 76 2e 1c 8f	..\$.&...~...v....	00001190	61 73 68 00 2e 64 79 6e	73 79 6d 00 2e 64 79 6e	..str..rel.plt..te
000011b0	b4 03 1d 7d 12 3f 0f 6e 54 37 57 c6 4b 76 3c cf	...j..?..nT7M.Kv6.	000011a0	73 74 72 00 2e 72 65 6c	2e 70 6c 74 00 2e 74 65	..xt..rodata.prel
000011c0	4d 45 94 e9 7c 47 be da 55 c7 63 c0 99 ce 45 77	..E..lG..U.c...Ew	000011b0	78 74 00 2e 72 6f 64 61	74 61 00 2e 70 72 65 69	..init.array..init_
000011d0	83 38 ff 2e 50 89 c0 92 1c f2 ae af 96 44 6f 6f	C8..P.....Do	000011c0	6e 69 74 5f 61 72 72 61	79 00 2e 69 6e 69 74 5f	..array..fini_arra
000011e0	49 96 c2 61 66 c6 40 e8 fe 6a 44 2c 54 88 e7 d8	..I..af..B...jD.T...	000011d0	61 72 72 61 79 00 2e 66	69 6e 69 5f 61 72 72 61	..y..ctors..dynam
000011f0	17 aa c1 92 7e 9b 4c f8 05 67 7e 19 53 0c 06 0f	...L...g...S....	000011e0	79 00 2e 63 74 6f 72 73	00 2e 64 79 6e 61 6d 69	..c..got..bss..co
00001200	cf b4 0d 33 46 8e da 73 49 e0 05 ef 9d 9e fc 0c	...3F...eI.....	000011f0	63 00 2e 67 6f 74 00 2e	62 73 73 00 2e 63 6f 6d	..ment..ARM.attrib
00001210	a3 93 c5 b5 38 75 96 40 22 43 74 5c 28 da 12 86	...8u...C.....	00001200	5d 65 6e 74 00 2e 41 52	4d 2e 61 74 74 72 69 62	
00001220	00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001210	5f 31 55 33 58 38 42 38	00 58 38 53 60 58 38 53	
00001230	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001240	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001250	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001260	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001270	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001280	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001290	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
000012a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
000012b0	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
000012c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
000012d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
000012e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
000012f0	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001300	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001310	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001320	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001330	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001340	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001350	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001360	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001370	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001380	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001390	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
000013a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
000013b0	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
000013c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
000013d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
000013e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
000013f0	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001400	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001410	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001420	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001430	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001440	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001450	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001460	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001470	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001480	00 00 00 00 00 00 00 00 00 00 00 00 00 00					
00001490	00 00 00 00 00 00 00 00 00 00 00 00 00 00					

Relevance in Android Security?

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





00001160	8d eb 6b 46 bf e2 2b 0e	13 f5 5e 93 85 ca 1f da	.k.f.+.+.+.+.	00001150	30 00 41 28 00 00 00 61	65 61 62 69 00 01 1e 00	0.A ...aeebi....
00001170	5c c5 e8 1f 15 cc d2 86	78 13 07 1e 4d f4 63 c7	.+.+.+.x...M.c.	00001160	00 00 05 35 54 45 00 06	04 08 01 09 01 12 04 14	...5FE.....
00001180	89 61 80 06 96 46 59 d0	33 4f ad 0c 1b aa 0e 85	.+.+.+.P.Y.3D....	00001170	01 15 01 17 03 18 01 19	01 1a 02 00 2e 73 68 73	...shs.....
00001190	61 08 a1 9e 99 5e d9 19	63 81 ab 54 05 05 92 8d	.a...+.+.TU....	00001180	74 72 74 61 62 00 2e 69	6e 74 65 72 70 00 2e 68	tntab..interp.h
000011a0	bf 2f 24 c2 b9 26 12 0f	02 22 9a 8e aa 76 2e 1c 8f	.\$.+.+.+.v....	00001190	61 73 68 00 2e 64 79 6e	73 79 69 00 2e 64 79 6e	ash..dynsym..dyn
000011b0	b4 03 1d 7d 12 3d 0f 0e	54 37 57 ca c6 46 76 3e cf	.+.+.?.nTm.Kv6..	000011a0	73 74 72 00 2e 72 65 6c	2e 70 6c 74 00 2e 74 65	str..rel.plt..tel
000011c0	8d 45 94 e9 7c 47 be da	55 c7 63 c0 99 ce 45 77	.+.+. .G..U.c...Ew	000011b0	78 74 00 2e 72 6f 64 61	74 61 00 2e 70 72 65 69	xt..rodاتا..prei
000011d0	43 38 ff 2e 50 89 c0 92	1c f2 ae af 96 44 6f 6f	C8..P...+.+.Do	000011c0	6e 69 74 5f 61 72 72 61	79 00 2e 69 6e 69 74 5f	init..array..init
000011e0	49 96 c2 61 66 c6 40 e8	fe 6a 44 2c 54 88 e7 d8	.+.+.f...jD.T...	000011d0	61 72 72 61 79 00 2e 66	69 6e 69 5f 61 72 72 61	array..fini..arra
000011f0	17 aa c1 92 7e 9b 4c f8	05 67 7c 19 53 c0 06 0f	.+.+.f...L...S...	000011e0	79 00 2e 63 74 6f 72 73	00 2e 64 79 6e 61 6d 69	y..ctors..dynami
00001200	cf b4 0d 33 46 8e da 73	49 e0 05 ef 9d 9e fc 0c	.+.+.f...f...l...	000011f0	63 00 2e 6f 6f 74 00 2e	62 73 73 00 2e 63 6f 6d	c...got..bss..com
00001210	a3 83 c5 b5 38 75 96 f0	22 43 74 5f 98 da 12 be	.+.+.8u...C...N...	00001200	6d 65 6e 74 00 2e 41 52	4d 2e 61 74 72 69 62	ment..ARM.attrib
00001220	de 67 3b 6b 02 b3 70 4a	90 18 04 66 03 20 01 1e	.g k..p.J....	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	76 29 3c 26 e6 ee 85 32	02 11 e5 a4 a4 1f 3a 78	v (<...2...:x	*			
00001250	36 42 1f 5a 24 86 1f 9e	33 35 ff 82 b3 d6 d5 2e	68.Z\$...35...x	00001240	0b 00 00 00 01 00 00 00	02 00 00 00 d4 80 00 00	
00001260	a4 c5 b5 20 a4 b4 1d 8d	14 00 00 00 00 00 00 00	.+.+.+.+.+.+.+.	00001250	44 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001270							
00001280							
00001290							
000012a0							
000012b0							
000012c0							
000012d0							
000012e0							
000012f0	8b 3a bf 33 8e 67 ea 84	af ab f8 14 56 1d 40 82	.+.+.g...+.V.E.	000012e0	29 00 00 00 09 00 00 00	02 00 00 00 bc 84 00 00	).....
00001300	ef 28 b7 3c 8d c1 a0 b8	07 8b 8f d2 a6 86 96 73	.+.+.+.+.+.+.s	000012f0	bc 04 00 00 98 00 00 00	03 00 00 00 06 00 00 00	
00001310	b2 c3 ad 4f 58 07 9a 9c 81	07 f9 4a b5 94 92 2b 67	.+.+.+.+.J...+g	00001300	04 00 00 00 08 00 00 00	2d 00 00 00 01 00 00 00	
00001320	04 b7 46 ae ef ab 9a 17	04 79 ed 97 d5 95 1e c2	.+.+.F...+.+.+.	00001310	06 00 00 00 54 85 00 00	54 05 00 00 f8 00 00 00	T...T...
00001330	e2 74 73 f4 0a 33 ca c5	4e 10 65 bd 02 09 4d e2	.+.+.+.S..N.e...K	00001320	00 00 00 00 00 00 00 00	04 00 00 00 04 00 00 00	
00001340	64 1b ec dd b8 ab 1e 12	50 a3 a4 65 17 86 15 6b	.+.+.+.J...S...c.	00001330	32 00 00 00 01 00 00 00	06 00 00 00 50 86 00 00	2.....
00001350	8f 59 1b 0c 47 d8 69 bb	41 48 e2 c9 b5 e3 63 6a	.+.+.V..J...AH...c.	00001340	50 06 00 00 e8 02 00 00	00 00 00 00 00 00 00 00	P.....f...
00001360	85 a7 1c 32 55 24 de d1	e2 84 cc b9 1e 7d 91 de	.+.+.ZUS...+.+.+.	00001350	10 00 00 00 00 00 00 00	38 00 00 00 01 00 00 00	8...
00001370	af 55 9f 06 0e 0b 9a c8	89 64 21 61 62 6e d6 d6	.+.+.U...+.+.d ab..	00001360	32 00 00 00 38 89 00 00	38 09 00 00 e0 02 00 00	2...8...8...
00001380	df 6f cf 51 ee 1d 9b c8	32 15 2b d9 42 c5 53 91	.+.+.Q...2...+..B.S.	00001370	00 00 00 00 00 00 00 00	04 00 00 00 01 00 00 00	
00001390	01 09 2a c2 9e 1e 85 93	59 9f e6 cf 18 7d 20 29	.+.+.K...+.Y...+..	00001380	40 00 00 00 10 00 00 00	03 00 00 00 00 90 00 00	@.....
000013a0	4b 16 1c 08 cb f2 7f 66	54 aa a3 84 91 e5 4f 79 95	.+.+.K...+.FT...E...	00001390	00 10 00 00 08 00 00 00	00 00 00 00 00 00 00 00	
000013b0	5e 15 f4 f6 fc bd 05 60	fd d5 6f 1f 16 bc 1a fe	.+.+.+.+.+.+.o.n...	000013a0	01 00 00 00 00 00 00 00	4f 00 00 00 0e 00 00 00	0...
000013c0	1a 17 83 0e b6 9c 17 0c	84 ad 3c 2d 03 ff 1a 82	.+.+.+.+.+.+.<...<	000013b0	03 00 00 00 08 90 00 00	08 10 00 00 08 00 00 00	
000013d0	93 e2 73 ca 55 ed d0 ba	6e f0 58 08 bf 09 77 8b	.+.+.W.U...n.X...w...	000013c0	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00	
000013e0	e1 dd 6b 6d 77 27 1e 05	25 42 4c b5 66 95 79 b6	.+.+.k.mw...*.KL-F-y...	000013d0	5b 00 00 0f 0f 00 00 00	03 00 00 00 10 90 00 00	[.....
000013f0	0a 3a 48 71 28 81 d6 11	74 48 5e a1 f3 e4 e9 27	.+.+.h.Q...+.th...+..	000013e0	10 10 00 00 08 00 00 00	00 00 00 00 00 00 00 00	
00001400	6d 8e 44 52 e4 bb 4c 42	a5 ba 9e c7 68 1e f5 ab	.+.+.m.DR...+.B...+.h...	000013f0	01 00 00 00 00 00 00 00	67 00 00 00 01 00 00 00	g...
00001410	1a 17 83 0e b6 9c 17 0c	84 ad 3c 2d 03 ff 1a 82	.+.+.+.+.+.+.<...<	00001400	03 00 00 00 18 90 00 00	18 10 00 00 08 00 00 00	
00001420	ff c9 33 80 75 3b 30 33	ce bc 00 cc 0c 7d 4c 4c	.+.+.3..u03...+.L...	00001410	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00	
00001430	d4 21 47 c5 af 03 de 0e	8a 2e 8c 91 00 c8 db da	.+.+. .G...+.+.p...	00001420	6e 00 00 00 06 00 00 00	03 00 00 00 20 90 00 00	n.....
00001440	48 f9 9e 18 08 e8 26 b9	f7 aa 0e 47 01 5c d2 43	.+.+.H...&...&...G.C	00001430	20 10 00 00 c8 00 00 00	04 00 00 00 00 00 00 00	
00001450	fd 5f 0f ca ee cc c3 df	b2 59 95 15 31 55 d0 51	.+.+.+.+.+.+.Y...1U.Q	00001440	04 00 00 00 08 00 00 00	77 00 00 00 01 00 00 00	
00001460	04 b7 46 ae ef ab 9a 17	d4 79 ed 97 d5 95 1e c2	.+.+.+.+.+.+.F...+.	00001450	03 00 00 00 e8 90 00 00	e8 10 00 00 58 00 00 00	
00001470	4c 8d 7f 6c dd 36 47	09 66 a5 ad 66 8b e1 8d	.+.+.L..u.1.6...F...f...	00001460	00 00 00 00 00 00 00 00	04 00 00 00 04 00 00 00	
00001480	c2 70 23 47 03 b7 9d	92 d2 59 09 b3 c0 68 b8	.+.+.p.G...+.Y...h...	00001470	7c 00 00 00 08 00 00 00	03 00 00 00 40 91 00 00	
00001490	21 60 5c 10 a9 8e 7b f0	43 32 93 27 7f 18 82 53	.+.+.I\...+.C2...+.S	00001480	40 11 00 00 10 00 00 00	00 00 00 00 00 00 00 00	8.....

Pangxie



```
00001160 8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da |..kF...+...^....| 00001150 30 00 41 28 00 00 00 61 65 61 62 69 00 01 1e 00 |0.A[...aeabi....|
00001170 5c c5 e8 1f 15 c0 d2 86 78 13 07 1e 4d f4 63 c7 |\\.....x...M.c.| 00001160 00 00 05 35 54 45 00 06 04 08 01 09 01 12 04 14 |...5TE.....sbs
00001180 89 61 80 06 96 46 59 0d 33 4f ad 0c 1b aa 0a 85 |.a...FY.30.....| 00001170 01 15 01 17 03 18 01 19 01 1a 02 00 2e 73 68 73 |ttrtab.interp.h
00001190 61 08 a1 9a 99 5e d9 19 fc 81 be 54 55 d5 92 8d |a...^.....TU...| 00001180 74 72 74 61 62 00 2e 69 6e 74 65 72 70 00 2e 68 |trtab.interp.h
000011a0 fb 2f 24 c2 b9 26 0d 02 22 9a 8a 76 2e 1c 8f |./$.&.....v...| 00001190 61 73 68 00 2e 64 79 6e 73 79 6d 00 2e 64 79 6e |lash.dynsym.dyn
000011b0 b4 03 1d 7d 12 3f 0f 6e 54 37 57 c6 4b 76 36 cf |...}.?..nT7M.Kv6.| 000011a0 73 74 72 00 2e 72 65 6c 2e 70 6c 74 00 2e 74 65 |str..rel.plt.te
000011c0 8d 45 94 e9 7c 47 be da 55 c7 63 c0 99 ee 45 72 |.F..IG..U...Fw| 000011b0 78 74 00 2e 72 6f 64 61 74 61 00 2e 70 72 65 69 |str..endata..prei
000011d0 |.....init_|
000011e0 |.....rma|
000011f0 |.....aml|
00001200 |.....com|
00001210 |.....rib|
00001220 |.....|
00001230 |.....|
00001240 |.....|
00001250 |.....|
00001260 |.....|
00001270 |.....|
00001280 |.....|
00001290 |.....|
000012a0 |.....|
000012b0 |.....|
000012c0 |.....|
000012d0 |.....|
000012e0 |.....|
000012f0 |.....|
00001300 |.....|
00001310 |.....|
00001320 |.....|
00001330 |.....|
00001340 |.....|
00001350 |.....|
00001360 |.....|
00001370 |.....|
00001380 |.....|
00001390 |.....|
000013a0 |.....|
000013b0 |.....|
000013c0 |.....|
000013d0 |.....|
000013e0 |.....|
000013f0 |.....|
00001400 |.....|
00001410 |.....|
00001420 |.....|
00001430 |.....|
00001440 |.....|
00001450 |.....|
00001460 |.....|
00001470 |.....|
00001480 |.....|
00001490 |.....|
```

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">
```



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'
- ▶ WrapperApplication.class
 - ▶ Loads library 'nsecure.so'
 - ▶ Calls native function **validate**

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

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

00001160	8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da	..kF...+...^....	00001150	30 00 41 28 00 00 00 61	65 61 62 69 00 01 1e 00	0.A[...aeabi....
00001170	5c c5 e8 1f 15 c0 d2 86 78 13 07 1e 4d f4 63 c7	\.....x...M.c.	00001160	00 00 05 35 54 45 00 06	04 08 01 09 01 12 04 14	...5TE.....
00001180	89 61 80 06 96 46 59 0d 33 4f ad 0c 1b aa 0a 85	.a...FY.30.....	00001170	01 15 01 17 03 18 01 19	01 1a 02 00 2e 73 68 73	shs
00001190	61 08 a1 9a 99 5e d9 19 fc 81 be 54 55 d5 92 8d	a.....TU....	00001180	74 72 74 61 62 00 2e 69	6e 74 65 72 70 00 2e 68	trtab..interp.h
000011a0	fb 2f 24 c2 b9 26 0d 02 22 9a 8a 76 2e 1c 8f	./\$.&...".v....	00001190	61 73 68 00 2e 64 79 6e	73 79 6d 00 2e 64 79 6e	lash..dynsym..dyn
000011b0	64 03 14 74 12 76 0c 6a 84 32 83 26 4b 78 8f	..3..&T30.k66	000011a0	73 74 72 00 2e 73 68 6e	2e 70 6e 74 00 2e 74 65	letp..rel.plt..te
000011c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000011b0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	onei
000011d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000011c0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	lit_
000011e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000011d0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	rna
000011f0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000011e0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	ami
00001200	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000011f0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	com
00001210	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001200	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	rib
00001220	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001210	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00001230	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001220	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00001240	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001230	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00001250	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001240	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00001260	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001250	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00001270	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001260	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00001280	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001270	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00001290	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001280	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000012a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001290	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000012b0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000012a0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000012c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000012b0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000012d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000012c0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000012e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000012d0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000012f0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000012e0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00001300	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000012f0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00001310	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001300	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00001320	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001310	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00001330	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001320	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00001340	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001330	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00001350	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001340	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00001360	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001350	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00001370	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001360	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00001380	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001370	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00001390	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001380	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000013a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001390	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000013b0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000013a0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000013c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000013b0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000013d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000013c0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000013e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000013d0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
000013f0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000013e0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	...
00001400	c2 70 23 47 03 b7 9d 88 92 d2 59 09 b3 c0 68 b8	..p#G.....Y...h.	00001470	7c 00 00 00 08 00 00 00	03 00 00 00 40 91 00 00	8
00001410	21 60 5c 10 a9 8e 7b 0f 43 32 93 27 7f 18 82 53	!'\....{.C2.'...S	00001480	40 11 00 00 10 00 00 00	00 00 00 00 00 00 00 00	8.....
00001420	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001490	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001430	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000014a0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001440	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000014b0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001450	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000014c0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001460	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000014d0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001470	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000014e0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001480	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		000014f0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001490	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		00001500	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	

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
verifyDqest	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_wrapper_WrapperApplication_validate
Java_com_merry_wrapper_WrapperApplication_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_wrapper_Wap
    MOVS    R1,R5
    MOVS    R0,R4
    BL      decryptDex
    MOVS    R0,R4
    BL      classDestroy
    POP     {R3-R5,PC}
; End of function Java_com_merry_wrapper_WrapperApplication_validate
```



00001160	8d eb 6b 46 bf e2 2b 0e	13 f5 5e 93 85 8c 1f da	.kf.+.^.....	00001150	30 00 41 28 00 00 00 61	65 61 62 69 00 01 1e 00	0.A[...aeebi....
00001170	5c c5 e8 1f 15 c0 d2 86	78 13 07 1e 4d f4 63 c7	.b.....x...M.c.	00001160	00 00 05 35 54 45 00 06	04 08 01 09 01 12 04 14	...5TE.....
00001180	89 61 80 06 96 46 59 d0	33 4f ad 0c 1b aa 0e 85	.b.....PY.3D.....	00001170	01 15 01 17 03 18 01 19	01 1a 02 00 2e 73 68 73	shs
00001190	61 08 a1 9e 99 5e d9 19	78 81 be 54 05 92 8d	a.....TU.....	00001180	74 72 74 61 62 00 2e 69	6e 74 65 72 70 2e 2e 68	trtab.interp.h
000011a0	bf 2f 24 c2 b9 26 d0 02	22 9a 8e aa 76 2e 1c 8f	./\$.b.....v.....	00001190	61 73 68 00 2e 64 79 6e	73 79 6d 00 2e 64 79 6e	ash.dynsym.dyn
000011b0	b4 03 1d 7d 12 32 0f 6e	54 37 57 c6 46 76 3c cf	.j.....nTm.Kv6..	000011a0	73 74 72 00 2e 72 65 6c	2e 70 6c 74 00 2e 74 65	str.rel.plt.te
000011c0	8d 45 94 9e 7c 47 be da	55 c7 63 c0 99 ce 45 77	.E.. G..U.c...Ew	000011b0	78 74 00 2e 72 6f 64 61	74 61 00 2e 70 72 65 69	xt..rodatab.prei
000011d0	43 38 ff 2e 50 89 c0 92	1c f2 ae af 96 44 6f	C8..P.....Do	000011c0	6e 69 74 5f 61 72 72 61	79 00 2e 69 6e 69 74 5f	nit.array.init_
000011e0	49 96 c2 61 66 c6 40 e8	6e 6a 44 2c 54 88 e7 d8	.l..af..jD.T...	000011d0	61 72 72 61 79 00 2e 66	69 6e 69 5f 61 72 72 61	array.fini.arra
000011f0	17 aa c1 92 7e 9b 4c f8	05 67 7e 19 53 0c 06 0f	.W.....L.g...S..	000011e0	79 00 2e 63 74 6f 72 73	00 2e 64 79 6e 61 6d 69	y..ctors.dynami
00001200	cf b4 0d 33 46 8e da 73	49 e0 05 ef 9d 9e fc 0c	.f.....f.....	000011f0	63 00 2e 67 6f 74 00 2e	62 73 73 00 2e 63 6f 6d	c...got..bss.com
00001210	a3 83 c5 b5 38 75 96 40	22 43 7f 5c f8 da 12 b6	8u..C.X.....	00001200	6d 65 6e 74 00 2e 41 52	4d 2e 61 74 72 72 69 62	ment..ARM.attrib
00001220	de 67 3b 6b 02 b3 70 4a	90 18 04 66 03 20 01 1e	.g;k..pJ.....	00001210	75 74 65 73 00 00 00 00	00 00 00 00 00 00 00 00	utes.....
00001230	*			00001220	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001240	76 29 3c 26 e6 ee 85 32	02 11 e5 a4 a4 1f 3a 78	v <.....:x	00001230	*		
00001250	36 42 f1 5a 24 86 1f 9e	33 95 ff 82 b3 d6 d5 2e	68.Z\$.....35.....	00001240	0b 00 00 00 01 00 00 00	02 00 00 00 d4 80 00 00	
00001260	ae b6 f6 20 c4 b2 44 8d	1f 90 c0 f4 a8 d2 2f f7	D...../	00001250	d4 00 00 00 13 00 00 00	00 00 00 00 00 00 00 00	
00001270	16 89 a2 ef c5 25 70 ff	9a d6 fb 4b a9 58 c4 b2	8p.....K.X..	00001260	01 00 00 00 00 00 00 00	13 00 00 00 05 00 00 00	
00001280							
00001290							
00001300							
00001310							
00001320							
00001330							
00001340							
00001350	8f 29 1b 8u 4a c7 d8 b9	bb 41 45 d2 e9 e3 b3 6a	.Y..J..RH...C..	00001340	50 00 00 00 e8 02 00 00	00 00 00 00 00 00 00 00	F.....
00001360	85 a7 1c 32 55 24 de d1	e2 84 cc b9 1e 7d 91 de	...2US.....	00001350	10 00 00 00 00 00 00 00	38 00 00 00 01 00 00 00	F.....8.....
00001370	af 55 9f 5e 06 9a c8 3e	89 64 21 61 62 f6 d6 d6	.U..^...dtab...	00001360	32 00 00 00 38 89 00 00	38 09 00 00 e0 02 00 00	2...8...8.....
00001380	df 6f cf 51 ee 1d 9b c8	32 15 2b d9 42 c5 53 91	.o.Q.....2+..B.S..	00001370	00 00 00 00 00 00 00 00	04 00 00 00 01 00 00 00	@.....
00001390	01 09 2a c2 9e 1e 85 93	59 ff e6 cf 18 7d 20 29	K.....Y.....	00001380	40 00 00 00 10 00 00 00	03 00 00 00 00 90 00 00	@.....
000013a0	4b b6 1c d8 cb f2 7f 66	54 aa a3 84 91 e5 f7 95	.K.....Y.....	00001390	00 10 00 00 08 00 00 00	00 00 00 00 00 00 00 00	@.....
000013b0	5e f5 fa 73 06 d8 05 60	fd d5 6f 1f fe bc 1a 8e	^.....o.n.....	000013a0	01 00 00 00 00 00 00 00	4f 00 00 00 0e 00 00 00	@.....
000013c0	1a 17 83 0e b6 9c 17 0c	84 ad 3c 2d 03 ff 1a 82	<.....<.....	000013b0	03 00 00 00 08 90 00 00	08 10 00 00 08 00 00 00	@.....
000013d0	93 e2 77 ca 55 ed 0a 6e	f0 58 08 bf 09 77 8b	.w.U.....X...w..	000013c0	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00	@.....
000013e0	e1 dd 6b 6d 77 27 1e 25	42 4b 4c b5 66 95 79 b6	.kmm^...*KL-F-y..	000013d0	5b 00 00 00 0f 00 00 00	03 00 00 00 10 90 00 00	@.....
000013f0	0e 3a 48 71 28 81 d6 11	74 48 5e a1 f3 e4 e9 27	.Hq.....TH.....	000013e0	10 10 00 00 08 00 00 00	00 00 00 00 00 00 00 00	@.....
00001400	6d 8e 44 52 e4 bb 4c 42	ae 5a ba 9e c7 68 1e f5 ab	m.DR...B...h...	000013f0	01 00 00 00 00 00 00 00	67 00 00 00 01 00 00 00	@.....g.....
00001410	1a 17 83 0e b6 9c 17 0c	84 ad 3c 2d 03 ff 1a 82	<.....<.....	00001400	03 00 00 00 18 90 00 00	18 10 00 00 08 00 00 00	@.....
00001420	ff c9 33 00 75 3b 30 33	ce bc 00 cc 0c 07 d6 4c	.3.uq03.....L..	00001410	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00	@.....
00001430	d4 21 47 c5 af 03 de e0	8a 2e 8c 91 70 c8 db da	.G.....p.....	00001420	6e 00 00 00 06 00 00 00	03 00 00 00 20 90 00 00	@.....n.....
00001440	48 f9 9e 18 d8 e8 26 b9	f7 aa 0e 47 01 5c d2 43	H.....&.....G..C	00001430	20 10 00 00 c8 00 00 00	04 00 00 00 00 00 00 00	@.....
00001450	fd 5f 0f ca ee cc c3 df	b2 59 95 15 31 55 d0 51	.W.....Y...1U.Q	00001440	04 00 00 00 08 00 00 00	77 00 00 00 01 00 00 00	@.....
00001460	04 b7 46 ef af 8b 9a 17	4d 79 ed 97 d5 95 1e c2	.F.....	00001450	03 00 00 00 e8 90 00 00	e8 10 00 00 58 00 00 00	@.....
00001470	4c 8d 75 fc 6d 36 47	09 66 af ad 66 8b e1 8d	.u.u.l.g..Y..f..	00001460	00 00 00 00 00 00 00 00	04 00 00 00 04 00 00 00	@.....
00001480	c2 70 23 47 03 bf 9d 88	92 d2 59 09 b3 c0 68 b8	.pBg.....Y..h...	00001470	7c 00 00 00 08 00 00 00	03 00 00 00 40 91 00 00	@.....
00001490	21 60 5c 10 a9 8e 7b 0f	43 32 93 27 7f 18 82 83	Y\.....C2.....S	00001480	40 11 00 00 10 00 00 00	00 00 00 00 00 00 00 00	@.....

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, =(a01234567890123-0x4B881D3C)
.text:4B881D38      ADD     R2, PC      "0123456789012345" =KEY
.text:4B881D3A      BL      AESDecrypt
.text:4B881D3E      POP     {R3,PC}
.text:4B881D3E      ; End of function digestDecrypt
.text:4B881D3E

```




```

00001160 8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da |...kf...+...^....| 00001150 30 00 41 28 00 00 00 61 65 61 62 69 00 01 1e 00 |0.A[...aeabi....|
00001170 5c c5 e8 1f 15 c0 d2 8e 78 13 07 1e 4d f4 63 c7 |...x...M.c...| 00001160 00 00 05 35 54 45 00 06 04 08 01 09 01 12 04 14 |...5TE.....|
00001180 89 61 80 06 96 46 59 d0 33 4f ad 0c 1b aa 0e 85 |...FY.3D...| 00001170 01 15 01 17 03 18 01 19 01 1a 02 00 2e 73 68 73 |...shs.....|
00001190 61 08 a1 9e 99 5e d9 19 fc 81 be 54 55 d5 92 8d |a...TU...| 00001180 74 72 74 61 62 00 2e 69 6e 74 65 72 70 00 2e 68 |trtab.interp.h|
000011a0 fb 2f 24 c2 b9 26 d0 d2 22 9a 8e aa 76 2e 1c 8f |$.&.v...| 00001190 61 73 68 00 2e 64 79 6e 73 79 6d 00 2e 64 79 6e |ash.dynsym.dyn|
000011b0 b4 03 1d 7d 12 3f 0f 6e 54 37 57 c6 4b 76 36 cf |...7.nT7M.Kv6.| 000011a0 73 74 72 00 2e 72 65 6c 2e 70 6c 74 00 2e 74 65 |str.rel.plt.te|
000011c0 4d 45 94 e9 7c 4f d4 da 55 c7 63 c0 99 ce 45 77 |.E..IG..U.c...Ew| 000011b0 78 74 00 2e 72 6f 64 61 74 61 00 2e 70 72 65 69 |xt..rodatab.prei|
000011d0 83 38 ff 2e 50 89 c0 92 1c f2 ae af 96 44 6f |C8..P.....Do| 000011c0 6e 69 74 5f 61 72 72 61 79 00 2e 69 6e 69 74 5f |init.array.init_|
000011e0 49 96 c2 61 66 ce 4c f8 05 64 44 2c 54 88 e7 d8 |l..af..B..Q.T...| 000011d0 61 72 72 61 79 00 2e 66 69 6e 69 5f 61 72 72 61 |array..fini_arra|
000011f0 17 aa c1 92 7e 9b 4c e8 fe 67 78 19 53 c0 06 0f |...L.g...S...| 000011e0 79 00 2e 63 74 6f 72 73 00 2e 64 79 6e 61 6d 69 |y..ctors.dynam|
00001200 cf b4 d0 33 46 8e da 73 49 e0 05 ef 9d 9e fc c0 |...3F..l...| 000011f0 63 00 2e 67 6f 74 00 2e 62 73 73 00 2e 63 6f 6d |c..got..bss.com|
00001210 a3 93 c5 b5 38 75 96 f0 22 43 7f 5c f9 da 12 b6 |...8d...C.....| 00001200 6d 65 6e 74 00 2e 41 52 4d 2e 61 74 72 69 62 |ment..ARM.attrib|
00001220 *
00001230
00001240
00001250
00001260
00001270
00001280
00001290
000012a0
000012b0
000012c0
000012d0
000012e0
000012f0
00001300 e2 74 73 f4 0a 33 ca c2 4e 10 65 bd b2 09 df 25 |...ts..3.N.e...X| 00001320 00 00 00 00 00 00 00 00 04 00 00 00 04 00 00 00 |...F.....|
00001310 64 1b ec dd b8 ab 1e 12 50 a3 ad 55 17 86 15 6b |...d...P...e...k| 00001310 32 00 00 00 01 00 00 00 06 00 00 00 50 86 00 00 |...2.....F...|
00001320
00001330
00001340
00001350
00001360
00001370
00001380
00001390
000013a0
000013b0
000013c0
000013d0
000013e0
000013f0
00001400
00001410
00001420
00001430
00001440
00001450
00001460
00001470
00001480
00001490

```

Unpacking

► verifyDigest()

- Reads asset file **diest**
- Calls decryption function

```
$ openssl enc -d -aes-128-ecb -nosalt -in diest -out diest.dec -K
30313233343536373839303132333435
```

```

00001160 8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da ..kF.+...^.... 00001150 30 00 41 28 00 00 00 61 65 61 62 69 00 01 1e 00 0.A[...aeabi....
00001170 5c c5 e8 4f 15 c0 d2 86 78 13 07 1e 4d f4 63 c7 \.....x...M.c. 00001160 00 00 05 35 54 45 00 06 04 08 01 09 01 12 04 14 ...5TE.....
00001180 89 61 80 06 96 46 59 0d 33 4f ad 0c 1b aa 0a 85 .a...FY.30..... 00001170 01 15 01 17 03 18 01 19 01 1a 02 00 2e 73 68 73 ...shs
00001190 61 08 a1 9e 99 5e d9 19 fc 81 be 54 55 d5 92 8d a.....TU... 00001180 74 72 74 61 62 00 2e 69 6e 74 65 72 70 00 2e 68 ttrtab.interp.h
000011a0 fb 2f 24 c2 b9 26 0d 02 22 9a 8e aa 76 2e 1c 8f ./$.&...".v... 00001190 61 73 68 00 2e 64 79 6e 73 79 6d 00 2e 64 79 6e ash.dynsym.dyn
000011b0 b4 03 14 74 12 36 0f 6e 54 37 57 c5 6b 76 36 cf . 2 cT7u kw6 000011a0 73 74 72 00 2e 72 65 6e 2e 70 6e 74 00 2e 74 65 tetr.cal.plt.te
000011c0 .. 000011b0 .. 000011c0 .. 000011d0 .. 000011e0 .. 000011f0 .. 00001200 .. 00001210 .. 00001220 .. 00001230 .. 00001240 .. 00001250 .. 00001260 .. 00001270 .. 00001280 .. 00001290 .. 000012a0 .. 000012b0 .. 000012c0 .. 000012d0 .. 000012e0 .. 000012f0 .. 00001300 .. 00001310 .. 00001320 .. 00001330 .. 00001340 .. 00001350 .. 00001360 .. 00001370 .. 00001380 .. 00001390 .. 000013a0 .. 000013b0 .. 000013c0 .. 000013d0 .. 000013e0 .. 000013f0 .. 00001400 .. 00001410 .. 00001420 .. 00001430 .. 00001440 .. 00001450 .. 00001460 .. 00001470 .. 00001480 .. 00001490 ..

```

Unpacking

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

```

000012c0 1a 17 83 0e b6 9c 17 0c 84 ad 3c 2d 03 ff 1a 82 .S.T1R3...<... 000012b0 02 00 00 00 b4 83 00 00 b4 03 00 00 05 01 00 00 ...
000012d0 .. 000012e0 .. 000012f0 .. 00001300 .. 00001310 .. 00001320 .. 00001330 .. 00001340 .. 00001350 .. 00001360 .. 00001370 .. 00001380 .. 00001390 .. 000013a0 .. 000013b0 .. 000013c0 .. 000013d0 .. 000013e0 .. 000013f0 .. 00001400 .. 00001410 .. 00001420 .. 00001430 .. 00001440 .. 00001450 .. 00001460 .. 00001470 .. 00001480 .. 00001490 ..

```

openssl enc -d -aes-128-ecb -nosalt -in diest -out diest.dec -K 30313233343536373839303132333435

Decrypted 'diest'

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



Static Analysis - libnsecure.so

- ▶ Exports
- ▶ Java_com_merry_wrapper_WrapperApplication_validate

```
EXPORT Java_com_merry_wrapper_WrapperApplication_validate
Java_com_merry_wrapper_WrapperApplication_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_wrapper_Wap
    MOVS    R1,R5
    MOVS    R0,R4
    BL      decryptDex ←
    MOVS    R0,R4
    BL      classDestroy
    POP     {R3-R5,PC}
; End of function Java_com_merry_wrapper_WrapperApplication_validate
```



00001160	8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da	.kf.+.^.....	00001150	30 00 41 28 00 00 00 61	65 61 62 69 00 01 1e 00	0.A[...aeebi....
00001170	5c c5 e8 1f 15 c0 d2 86 78 13 07 1e 4d f4 63 c7	x...M.c.	00001160	00 00 05 35 54 45 00 06	04 08 01 09 01 12 04 14	...5TE.....
00001180	89 61 80 06 96 96 46 59 0d 3c 4f ad 0c 1b aa 0e 85	PY.30....	00001170	01 15 01 17 03 18 01 19	01 1a 02 00 2e 73 68 73	...shs.....
00001190	61 08 a1 9e 99 5e d9 19 f3 81 be 54 05 92 8d	a.....TU.....	00001180	74 72 74 61 62 00 2e 69	6e 74 65 72 70 2e 2e 68	tstab.interp.h
000011a0	bf 2f 24 c2 b9 26 0d 02 22 9a 8e aa c6 26 1c 8f	./\$.&...v.....	00001190	61 73 68 00 2e 64 79 6e	73 79 6d 00 2e 64 79 6e	ash..dynsym..dyn
000011b0	b4 03 1d 7d 12 3f 0f 6e 54 37 57 c6 46 76 3e cf	.?.nTm.Kv6..	000011a0	73 74 72 00 2e 72 65 6c	2e 70 6c 74 00 2e 74 65	str..rel.plt..te
000011c0	8d 45 94 9f 7c 47 be da 55 c7 63 c0 99 ce 45 77	.E..IG..U.c...Ew	000011b0	78 74 00 2e 72 6f 64 61	74 61 00 2e 70 72 65 69	xt..rodata.prel
000011d0	43 38 ff 2e 50 89 c0 92 1c f2 ae af af 96 44 6f	C\$.P.....Do	000011c0	6e 69 74 5f 61 72 72 61	79 00 2e 69 6e 69 74 5f	init.array..init_
000011e0	49 96 c2 61 66 c6 40 e8 fe 6a 74 2c 54 88 e7 d8	I..af..E..JdT..	000011d0	61 72 72 61 79 00 2e 66	69 6e 69 5f 61 72 72 61	array..fini.arra
000011f0	17 aa c1 92 7e 9b 4c f8 05 6a 78 19 53 c0 06 0f	L.g...S..	000011e0	79 00 2e 63 74 6f 72 73	00 2e 64 79 6e 61 6d 69	y..ctors..dynami
00001200	cf b4 0d 33 46 8e da 73 49 e0 05 ef 9d 9e fc 0c	f..e.....	000011f0	63 00 2e 67 6f 74 00 2e	62 73 73 00 2e 63 6f 6d	c..got..bss.com
00001210	a3 83 c5 b3 85 75 96 40 22 43 7f 5c f8 da 12 b6	8u...C...	00001200	6d 65 6e 74 00 2e 41 52	4d 2e 61 74 74 72 69 62	ment..ARM.attrib
00001220	de 67 3b 6b 02 b3 70 4a 90 18 04 66 03 20 01 1e	.gik..pJ.....	00001210	75 74 65 73 00 00 00 00	00 00 00 00 00 00 00 00	utes.....
00001230	*		00001220	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001240	76 29 3c 26 e6 ee 85 32 02 11 e5 a4 a4 1f 3a 78	v(<.....2.....x	00001230	0b 00 00 00 01 00 00 00	02 00 00 00 d4 80 00 00	
00001250	36 42 1f 5a 24 86 1f 9e 33 35 ff 82 b3 d6 d5 2e	68.Z\$....35.....	00001240	04 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001260	aa b5 65 20 a4 b5 a4 4e 60 ce 05 00 00 00 00 00		00001250	04 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001270	0000		00001260	0000		
00001280	0000		00001270	0000		
00001290	0000		00001280	0000		
00001300	0000		00001290	0000		
00001310	0000		00001300	0000		
00001320	0000		00001310	0000		
00001330	0000		00001320	0000		
00001340	0000		00001330	0000		
00001350	0000		00001340	0000		
00001360	0000		00001350	0000		
00001370	8d 6f cf 51 ee 1d 9b c8 32 15 2b d9 42 c5 53 91	.o.Q.....2+..B.S.	00001370	00 00 00 00 00 00 00 00	04 00 00 00 01 00 00 00	
00001380	00 00 00 00 00 00 00 00		00001380	40 00 00 00 10 00 00 00	03 00 00 00 00 90 00 00	@.....
00001390	01 09 2a c2 9e 1e 85 93 59 f9 e6 cf 18 7d 20 29	.K.....Y.....	00001390	00 10 00 00 08 00 00 00	00 00 00 00 00 00 00 00	
000013a0	4b b6 1c 08 cb f2 7f 66 54 aa a3 84 91 45 f7 95		000013a0	01 00 00 00 08 00 00 00	4f 00 00 00 0e 00 00 00	
000013b0	5e f5 fa f6 fe 0b d0 05 60 fd d5 6f 1f fe bc 1a fe		000013b0	03 00 00 00 08 90 00 00	08 10 00 00 08 00 00 00	
000013c0	1a 17 83 0e b6 9c 17 0c 84 ad 3c 2d 03 ff 1a 82		000013c0	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00	
000013d0	93 e2 77 ca 55 ed d0 ba 6e f0 58 08 bf 09 77 8b		000013d0	00 00 00 00 0f 00 00 00	03 00 00 00 10 90 00 00	
000013e0	e1 dd 6b 6d 77 27 1e d5 22 4b 4c b5 66 95 79 b6		000013e0	10 10 00 00 08 00 00 00	00 00 00 00 00 00 00 00	
000013f0	0e 3a 48 71 28 81 d6 11 74 48 5e a1 f3 a4 e9 27		000013f0	01 00 00 00 00 00 00 00	67 00 00 00 01 00 00 00	
00001400	6d 8e 44 52 e4 bb c4 42 05 ba 9e c7 68 1e f5 ab	m.DR...B...h...	00001400	03 00 00 00 18 90 00 00	18 10 00 00 08 00 00 00	
00001410	1a 17 83 0e b6 9c 17 0c 84 ad 3c 2d 03 ff 1a 82		00001410	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00	
00001420	ff c9 33 00 75 3b 30 33 3c bc 00 cc 0c c7 da 4c		00001420	6e 00 00 00 06 00 00 00	03 00 00 00 20 90 00 00	
00001430	d4 21 47 c5 af 03 de e0 8a 2e 8c 91 70 d8 db da		00001430	20 10 00 00 c8 00 00 00	04 00 00 00 00 00 00 00	
00001440	48 f9 9e 18 d8 e8 c2 b9 f7 aa 9e 07 41 5c d2 43		00001440	04 00 00 00 08 00 00 00	77 00 00 00 01 00 00 00	
00001450	fd 5f 0f ca ee cc c3 df b2 59 95 15 31 55 d0 51		00001450	03 00 00 00 e8 90 00 00	e8 10 00 00 58 00 00 00	
00001460	04 b7 46 e6 ef ab 9a 17 d4 79 ed 97 d5 9e 1e c2		00001460	00 00 00 00 00 00 00 00	04 00 00 00 04 00 00 00	
00001470	4c 8d 75 fc 6c dd 36 47 09 66 a5 ad 66 8b e1 8d		00001470	7c 00 00 00 08 00 00 00	03 00 00 00 40 91 00 00	
00001480	c2 70 23 47 03 bf 9d 88 92 d2 59 09 b3 c0 68 b8		00001480	40 11 00 00 10 00 00 00	00 00 00 00 00 00 00 00	
00001490	21 60 5c 10 a9 8e 7b f0 43 32 93 27 7f 18 82 83		00001490	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	

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
```



```

00001160 8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da |.kf.+.^....| 00001150 30 00 41 28 00 00 00 61 65 61 62 69 00 01 1e 00 |0.A[...aeabi....|
00001170 5c c5 e8 1f 15 c0 d2 86 78 13 07 1e 4d f4 63 c7 | \.....x...M.c.| 00001160 00 00 05 35 54 45 00 06 04 08 01 09 01 12 04 14 |...5TE.....shs|
00001180 89 61 80 06 96 46 59 0d 33 4f ad 0c 1b aa 0e 85 |.B...FY.3D....| 00001170 01 15 01 17 03 18 01 19 01 1a 02 00 2e 73 68 73 |ttrtab.interp.h|
00001190 61 08 a1 9e 99 5e d9 19 fc 81 be 54 55 d5 92 8d |a.....TU....| 00001180 74 72 74 61 62 00 2e 69 6e 74 65 72 70 00 2e 68 |ttrtab.interp.h|
000011a0 fb 2f 24 c2 b9 26 0d 22 9a 8e aa 76 2e 1c 8f |./$.&..."v...| 00001190 61 73 68 00 2e 64 79 6e 73 79 6d 00 2e 64 79 6e |ash..dynsym..dyn|
000011b0 b4 03 1d 7d 12 3f 0f 6e 54 37 57 c6 4b 76 36 cf |...}.?..nTm.Kv6.| 000011a0 73 74 72 00 2e 72 65 6c 2e 70 6c 74 00 2e 74 65 |str..rel.plt..te|
000011c0 8d 45 94 9f 7c 47 be da 55 c7 63 c0 99 ce 45 77 |.E..[G...U.c...Ew| 000011b0 78 74 00 2e 72 6f 64 61 74 61 00 2e 70 72 65 69 |xt..rodata..prei|
000011d0 43 38 ff 2e 50 00 c9 12 c2 ae af 96 44 6f |C8..P.....Do| 000011c0 6e 69 74 5f 61 72 72 61 79 00 2e 69 6e 69 74 5f |nit_array..init_|
000011e0 49 96 c2 61 66 c6 40 e8 fe 6a 44 2c 54 88 e7 d8 |1..ef.B...j0,T...| 000011d0 61 72 72 61 79 00 2e 66 69 6e 69 5f 61 72 72 61 |array..fini_arra|
000011f0 |.....| 000011e0 |.....|
00001200 |.....| 000011f0 |.....|
00001210 |.....| 00001200 |.....|
00001220 |.....| 00001210 |.....|
00001230 |.....| 00001220 |.....|
00001240 |.....| 00001230 |.....|
00001250 |.....| 00001240 |.....|
00001260 |.....| 00001250 |.....|
00001270 |.....| 00001260 |.....|
00001280 |.....| 00001270 |.....|
00001290 |.....| 00001280 |.....|
000012a0 |.....| 00001290 |.....|
000012b0 |.....| 000012a0 |.....|
000012c0 |.....| 000012b0 |.....|
000012d0 |.....| 000012c0 |.....|
000012e0 |.....| 000012d0 |.....|
000012f0 |.....| 000012e0 |.....|
00001300 |.....| 000012f0 |.....|
00001310 |.....| 00001300 |.....|
00001320 |.....| 00001310 |.....|
00001330 |.....| 00001320 |.....|
00001340 |.....| 00001330 |.....|
00001350 |.....| 00001340 |.....|
00001360 |.....| 00001350 |.....|
00001370 |.....| 00001360 |.....|
00001380 |.....| 00001370 |.....|
00001390 |.....| 00001380 |.....|
000013a0 |.....| 00001390 |.....|
000013b0 |.....| 000013a0 |.....|
000013c0 |.....| 000013b0 |.....|
000013d0 |.....| 000013c0 |.....|
000013e0 |.....| 000013d0 |.....|
000013f0 |.....| 000013e0 |.....|
00001400 |.....| 000013f0 |.....|
00001410 |.....| 00001400 |.....|
00001420 |.....| 00001410 |.....|
00001430 |.....| 00001420 |.....|
00001440 |.....| 00001430 |.....|
00001450 |.....| 00001440 |.....|
00001460 |.....| 00001450 |.....|
00001470 |.....| 00001460 |.....|
00001480 |.....| 00001470 |.....|
00001490 |.....| 00001480 |.....|

```

Unpacking

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

Decrypted 'clex'

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



00001160	8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da	.kf.+.+.+.+.+.+. .00001150	30 00 41 28 00 00 00 61	65 61 62 69 00 01 1e 00	0.A[...aeabi....
00001170	5c c5 e8 1f 15 c0 d2 86 78 13 07 1e 4d f4 63 c7	.S....x...M.c. 00001160	00 00 05 35 54 45 00 06	04 08 01 09 01 12 04 14	...5TE.....
00001180	89 61 80 06 96 46 59 d0 33 4f ad 0c 1b aa 0e 85	.S...FY.3D..... 00001170	01 15 01 17 03 18 01 19	01 1a 02 00 2e 73 68 73	...shs
00001190	61 08 a1 9e 99 5e d9 19 fc 81 be 54 55 d5 92 8d	a.....v..... 00001180	74 72 74 61 62 00 2e 69	6e 74 65 72 70 00 2e 68	tatab..interp..h
000011a0	fb 2f 24 c2 b9 26 d0 02 22 9a 8e aa 76 2e 1c 8f	./\$.k...v..... 00001190	61 73 68 00 2e 64 79 6e	73 79 6d 00 2e 64 79 6e	ash..dynsym..dyn
000011b0	b4 03 1d 7d 12 3f 0f 6e 54 37 57 c6 4b 76 36 cf	./\$.?..nT7M.Kv6.. 000011a0	73 74 72 00 2e 72 65 6c	2e 70 6c 74 00 2e 74 65	str..rel.plt..te
000011c0	8d 45 94 e9 7c 47 8e da 55 c7 63 c0 99 ce 45 77	.E... G...U.c...Ew 000011b0	78 74 00 2e 72 6f 64 61	74 61 00 2e 70 72 65 69	xt..rodata..prei
000011d0	43 38 ff 2e 50 b9 c0 92 1c f2 ae af 96 44 6f	C8..P.....Do 000011c0	6e 69 74 5f 61 72 72 61	79 00 2e 69 6e 69 74 5f	nit.array..init_
000011e0	49 96 c2 61 66 c6 40 e8 fe 6a 44 2c 54 88 e7 d8	I..af..B...jD.T... 000011d0	61 72 72 61 79 00 2e 66	69 6e 69 5f 61 72 72 61	array..fini arra
000011f0	17 aa c1 92 7e 9b 4c f8 05 67 7e 19 53 0c 06 0f	L..g...S... 000011e0	79 00 2e 63 74 6f 72 73	00 2e 64 79 6e 61 6d 69	y..ctors..dynam
00001200	cf b4 0d 33 46 8e da 73 49 e0 05 ef 9d 9e fc 0c	...3F...el..... 000011f0	63 00 2e 67 6f 74 00 2e	62 73 73 00 2e 63 6f 6d	c..got..bss..co
00001210	a3 93 c5 b5 38 78 96 40 22 43 74 5c 83 da 12 b6	...8u...C\..... 00001200	6d 65 6e 74 00 2e 41 52	4d 2e 61 74 74 72 69 62	ment..ARM.attrib
00001220					
00001230					
00001240					
00001250					
00001260					
00001270					
00001280					
00001290					
000012a0					
000012b0					
000012c0					
000012d0					
000012e0					
000012f0					
00001300					
00001310					
00001320					
00001330					
00001340					
00001350					
00001360					
00001370					
00001380					
00001390					
000013a0					
000013b0					
000013c0					
000013d0					
000013e0					
000013f0					
00001400					
00001410					
00001420					
00001430					
00001440					
00001450					
00001460					
00001470					
00001480					
00001490					

Analyst Friendly

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



000011608d eb 6b 46 bf e2 2b 0e13 f5 5e 93 85 ca 1f da|.k.f.+.+.+.+.+.+.+.|0000115030 00 41 28 00 00 00 6165 61 62 69 00 01 1e 00|0.A[...+eabi....|

000011705c c5 e8 1f 15 cc d2 8678 13 07 1e 4d f4 63 c7|.+.+.+.+.+.+.+.+.+.|0000116000 00 05 35 54 45 00 0604 08 01 09 01 12 04 14|...5FE.....|

0000118089 61 80 06 96 46 59 0d33 4f ad 0c 1b aa 0e 85|.a.+.+.+.+.+.+.+.+.+.|0000117001 15 01 17 03 18 01 1901 1a 02 00 2e 73 68 73|...shs.....|

0000119061 08 a1 9e 99 5e d9 19fc 81 be 54 55 05 92 8d|a.+.+.+.+.+.+.+.+.+.|0000118074 72 74 61 62 00 2e 696e 74 65 72 70 00 2e 2e 68|trtab.interp.h|

000011a0bf 2f 24 c2 b9 26 1d 0222 9a 8e aa 76 2e 1c 8f|.j\$.+.+.+.+.+.+.+.+.|.0000119061 73 68 00 2e 64 79 6e73 79 6d 00 2e 64 79 6e|ash.dynsym.dyn|

000011b0b4 03 1d 7d 12 3f 0f 6e54 37 5f ad c6 76 3e cf|.+.+.+.+.+.+.+.+.+.|000011a073 74 72 00 2e 72 65 6c2e 70 6c 74 00 2e 74 65|str.rel.plt.tel|

000011c08d 45 94 9e 7c 47 be da55 c7 63 c0 99 ce 45 77|.E.+.G.+.U.+.c.+.Ew|000011b078 74 00 2e 72 6f 64 6174 61 00 2e 70 72 65 69|xt..rodata.prei|

000011d043 38 ff 2e 50 89 c0 921c f2 ae af 96 44 6f|C8.+.P.+.+.+.+.+.+.|000011c06e 69 74 5f 61 72 72 6179 00 2e 69 6e 69 74 5f|init.array.init|

000011e049 96 c2 61 66 c6 40 e8fe 6a 44 2c 54 88 e7 d8|.l.+.af.+.Q.T.+.+.+.|000011d061 72 72 61 79 00 2e 6669 6e 69 5f 61 72 72 61|array.fini.array|

000011f017 aa c1 92 7e 9b 4c f850 67 7b 19 53 c0 06 0f|.+.+.L.+.+.S.+.+.+.|000011e079 00 2e 63 74 6f 72 7300 2e 64 79 6e 61 6d 69|y.ctors.dynmal|

00001200cf b4 0d 33 46 8e da 7349 e0 05 ef 9d 9e fc 0c|.+.F.+.f.+.+.+.+.+.|000011f063 00 2e 67 6f 74 00 2e62 73 73 00 2e 63 6f 6d|c..got..bss.com|

00001210a3 83 c5 35 38 75 9e 4022 43 7f 5c f8 da 12 b6|.+.8u.+.C.+.+.+.+.|000012006d 65 6e 74 00 2e 41 524d 2e 61 74 72 69 62|ment..ARM.attrib|

00001220de 67 3b 6b 02 b3 70 4a90 18 04 66 03 20 01 1e|.g.k.+.p.J.+.+.+.+.|0000121075 74 65 73 00 00 00 0000 00 00 00 00 00 00 00|utes.....|

*0000122000 00 00 00 00 00 00 0000 00 00 00 00 00 00 00|.....|

0000124076 29 3c 26 e6 ee 85 3202 11 e5 a4 a4 1f 3a 78|v)(<...+...+...+x|*000012400b 00 00 00 01 00 00 0002 00 00 00 d4 80 00 00|.....|

0000125036 42 1f 5a 24 86 1f 9e33 95 cf 82 b3 d6 d5 2e|.68.Z\$...35.....|00001250da 00 00 00 43 00 00 0000 00 00 00 00 00 00 00|.....|

00001260ae b6 b6 20 c4 b2 44 8d1f 30 0f 4a a8 d2 2f 7f|.+.+.D.....+...|0000126000 00 00 00 00 00 00 0000 00 00 00 00 00 00 00|.....|

000012700

LIAPP


```

00001160 8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da |.kf.+.^....| 00001150 30 00 41 28 00 00 00 61 65 61 62 69 00 01 1e 00 |0.A[...aebi....|
00001170 5c c5 e8 1f 15 cc d2 8e 78 13 07 1e 4d f4 63 c7 | \.....x...M.c. | 00001160 00 00 05 35 54 45 00 06 04 08 01 09 01 12 04 14 |...5TE.....|
00001180 89 61 80 06 96 46 59 0d 33 4f ad 0c 1b aa 0e 85 | \.....PY.3D....| 00001170 01 15 01 17 03 18 01 19 01 1a 02 00 2e 73 68 73 |...shs.....|
00001190 61 08 a1 9e 99 5e 49 19 f3 81 be 54 55 d5 92 8d | a.....TU.....| 00001180 74 72 74 61 62 00 2e 69 6e 74 65 72 70 00 2e 68 |tstab.interp.h|
000011a0 fb 2f 24 c2 19 26 0d 02 22 9a 8e aa 76 2e 1c 8f | \$.&.....v....| 00001190 61 73 68 00 2e 64 79 6e 73 79 69 00 2e 64 79 6e |ash..dynsym..dyn|
000011b0 b4 03 1d 7d 12 3f 0f 6e 54 37 57 c6 4b 76 36 cf | \.?.nT7M.Kv6...| 000011a0 73 74 72 00 2e 72 65 6c 2e 70 6c 74 00 2e 74 65 |str..rel.plt..te|
000011c0 4d 45 94 9e 7c 47 8e da 55 c7 63 c0 99 ce 45 77 | \.E..G..U.c...Ew| 000011b0 78 74 00 2e 72 6f 64 61 74 61 00 2e 70 72 65 69 |xt..rodata..prei|
000011d0 83 38 ff 2e 50 b9 c0 92 1c f2 ae af 96 44 6f 6f | C8..P.....Do...| 000011c0 6e 69 74 5f 61 72 72 61 79 00 2e 69 6e 69 74 5f |init.array..init_|
000011e0 49 96 c2 61 66 c6 40 e8 fe 6a 44 2c 54 88 e7 d8 | l..af..B...Q,T...| 000011d0 61 72 72 61 79 00 2e 66 69 6e 69 5f 61 72 72 61 |array..fini arra|
000011f0 17 aa c1 92 7e 9b 4c f8 05 67 7e 19 53 0c 06 0f | \.....L.g...S...| 000011e0 79 00 2e 63 74 6f 72 73 00 2e 64 79 6e 61 6d 69 |y..ctors..dynam|
00001200 cf b4 0d 33 46 8a 73 49 e0 05 ef 9d 9e fc 0c | \...3F...l.....| 000011f0 63 00 2e 67 6f 74 00 2e 62 73 73 00 2e 63 6f 6d |c..got..bss..com|
00001210 a3 93 c5 b5 38 78 96 40 27 43 74 5c 49 da 17 b6 | \.....8u...f.....| 00001200 6d 65 6e 74 00 2e 41 82 4d 2e 61 74 74 72 69 6d |ment..@Bn.attrib|
00001220 *
00001230
00001240
00001250
00001260
00001270
00001280
00001290
00001300
00001310
00001320
00001330
00001340
00001350
00001360
00001370
00001380
00001390
00001400
00001410
00001420
00001430
00001440
00001450
00001460
00001470
00001480
00001490

```

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">

```



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);
    }
}

```



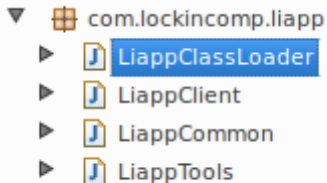
```

00001160 8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da |..kF...+...^....| 00001150 30 00 41 28 00 00 00 61 65 61 62 69 00 01 1e 00 |0.A[...aeabi....|
00001170 5c c5 e8 1f 15 c0 d2 86 78 13 07 1e 4d f4 63 c7 |N.....x...M.c..| 00001160 00 00 05 35 54 45 00 06 04 08 01 09 01 12 04 14 |...5TE.....|
00001180 89 61 80 06 96 46 59 0d 33 4f ad 0c 1b aa 0e 85 |.a...PY.30.....| 00001170 01 15 01 17 03 18 01 19 01 1a 02 00 2e 73 68 73 |.....shs|
00001190 61 08 a1 9e 99 5e d9 19 fc 8f be 54 55 d5 92 8d |a...^.....TU...| 00001180 74 72 74 61 62 00 2e 69 6e 74 65 72 70 00 2e 68 |trtab..interp.h|
000011a0 fb 2f 24 c2 b9 26 0d 02 22 9a 8e aa 76 2e 1c 8f |./$.&...^.....v...| 00001190 61 73 68 00 2e 64 79 6e 73 79 6d 00 2e 64 79 6e |lash..dynsym..dyn|

```

Static Analysis

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



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
```




00001160	8d eb 6b 46 bf e2 2b 0e	13 f5 5e 93 85 ca 1f da	..k.f+.+.+.+.+.+.+.+	00001150	30 00 41 28 00 00 00 61	65 61 62 69 00 01 1e 00	0.A[...+eabi....	
00001170	5c c5 e8 1f 15 cc d2 86	78 13 07 1e 4d f4 63 c7	..N...x...M.c...	00001160	00 00 05 35 54 45 00 06	04 08 01 09 01 12 04 14	...5fE.....	
00001180	89 61 80 06 96 46 59 d0	33 4f ab ad 01 ba aa 0e 85	..a...fY.30....	00001170	01 15 01 17 03 18 01 19	01 1a 02 00 2e 73 68 73	...shs.....	
00001190	61 08 a1 9e 99 5e d9 19	fc 81 be 5a 05 05 92 8d	..a...+.TU....	00001180	74 72 74 61 62 00 2e 69	6e 74 65 72 70 02 2e 68	..trtab..interp..h	
000011a0	bf 2f 24 c2 b9 26 1d 02	22 9a 8e aa 76 2e 1c 8f	..\$.B...v.....	00001190	61 73 68 00 2e 64 79 6e	73 79 6d 00 2e 64 79 6e	..ash..dynsym..dyn	
000011b0	b4 03 1d 7d 12 3f 0f 6e	54 37 5f c6 46 76 3e cf	..j..?..nT7M.Kv6..	000011a0	73 74 72 00 2e 72 65 6c	2e 70 6c 74 00 2e 74 65	..str..rel.plt..tel	
000011c0	8d 45 94 9e 7c 47 be da	55 c7 63 c0 99 ce 45 77	..E..IG..U.c...Ew	000011b0	78 74 00 2e 72 6f 64 61	74 61 00 2e 70 72 65 69	..xt..rodata..prei	
000011d0	43 38 ff 2e 50 89 c0 92	1c f2 ae af 96 44 6f	..C.E..P.....Do	000011c0	6e 69 74 5f 61 72 72 61	79 00 2e 69 6e 69 74 5f	..init..array..init..	
000011e0	49 96 c2 61 66 c6 40 e8	fe 6a 44 2c 54 88 e7 d8	..I..af...jD.T....	000011d0	61 72 72 61 79 00 2e 66	69 6e 69 5f 61 72 72 61	..array..fini..array	
000011f0	17 aa c1 92 7e 9b 4c f8	05 67 78 19 53 c0 06 0f	..+...L.B...S....	000011e0	79 00 2e 63 74 6f 72 73	00 2e 64 79 6e 61 62 69	..y..ctors..dynami	
00001200	cf b4 0d 33 46 8e da 73	49 e0 05 ef 9d 9e fc 0c	..3F...f.....	000011f0	63 00 2e 67 6f 74 00 2e	62 73 73 00 2e 63 6f 6d	..c..got..bss..com	
00001210	a3 83 c5 35 38 75 9e 40	22 43 7f 5c f8 da 12 b6	..8u...C...N....	00001200	6d 65 6e 74 00 2e 41 52	4d 2e 61 74 74 72 69 62	..ment..ARM.attrib	
00001220	de 67 3b 6b 02 b3 70 4a	90 18 04 66 03 20 01 1e	..g.k..p.J....	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	76 29 3c 26 e6 ee 85 32	02 11 e5 a4 a4 1f 3a 78	v)(<.....:x	*				
00001250	36 42 1f 5a 24 86 1f 9e	33 35 cf 82 b3 d6 d5 2e	68.Z\$...35....	00001240	0b 00 00 00 01 00 00 00	02 00 00 00 d4 80 00 00		
00001260	ae ba b6 20 c4 b2 44 8d	1f 90 0f 64 a8 d2 2f 7f	D...../..	00001250	da 00 00 00 13 00 00 00	00 00 00 00 00 00 00 00		
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....	000012a0	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00		
000012f0	8b 3a bf 33 8e 67 ea 84	af ab 8b 14 56 1d 40 82	3.g...f..E..	000012b0	29 00 00 00 09 00 00 00	02 00 00 00 bc 84 00 00		
00001300	ef 28 b7 3c 8d c1 a0 08	b7 8b fd a2 86 96 73	f.....s...	000012c0	bc 04 00 00 98 00 00 00	03 00 00 00 06 00 00 00		
00001310	b2 c3 af 58 07 9a 9c 81	07 f9 4a b5 94 92 2b 67	X...J...+g...	00001300	04 00 00 00 08 00 00 00	2d 00 00 00 01 00 00 00		
00001320	04 b7 46 ae ef ab 9a 17	4d 79 ed 97 d5 95 1e c2	F.....J....	00001310	06 00 00 00 54 85 00 00	54 05 00 00 f8 00 00 00	T..T....	
00001330	e2 74 73 f4 0a 33 ca c2	4e 10 65 bd b2 09 df 25	d...S..N.e...K	00001320	00 00 00 00 00 00 00 00	04 00 00 00 04 00 00 00		
00001340	64 1b ec dd b8 ab 1e 12	90 a3 a4 65 17 86 15 6b	V..J...S..H...c	00001330	32 00 00 00 01 00 00 00	06 00 00 00 50 86 00 00	2.....	
00001350	8f 59 1b 8c 47 cf d8 69	bb 41 48 d2 c8 b5 e3 6a	V..J...S..H...c	00001340	50 06 00 00 e8 02 00 00	00 00 00 00 00 00 00 00	P.....f...	
00001360	85 a7 1c 32 55 24 de d1	d2 84 cc b9 1e 7d 91 de	ZUS.....	00001350	10 00 00 00 00 00 00 00	38 00 00 00 01 00 00 00	8.....	
00001370	a5 55 9f 06 0e 0b 9a c8	89 64 21 61 62 6e d6 d6	U..Q...f..d..ab..	00001360	32 00 00 00 38 89 00 00	38 09 00 00 e0 02 00 00	2...8...8...	
00001380	df 6f cf 51 ee 1d 9b c8	32 15 2b d9 4d c2 53 91	Q...Q...2...+..B..S..	00001370	00 00 00 00 00 00 00 00	04 00 00 00 01 00 00 00		
00001390	01 09 2a c2 9e 1e 85 93	99 59 e6 cf 18 7d 20 29	K...*...Y...Y...)	00001380	40 00 00 00 10 00 00 00	03 00 00 00 90 00 00 00	@.....	
000013a0	4b 16 1c 08 cb f2 7f 66	54 aa a3 84 91 e5 47 f9 95	K...*...Y...Y...)	00001390	00 10 00 00 08 00 00 00	00 00 00 00 00 00 00 00		
000013b0	5e f5 f4 f6 fc 0b d5 05	6f d5 6f 1f 16 bc 1a fe	K...*...Y...Y...)	000013a0	01 00 00 00 00 00 00 00	4f 00 00 00 0e 00 00 00	0.....	
000013c0	1a 17 83 0e b6 9c 17 0c	84 ad 3c 2d 03 ff 1a 82	K...*...Y...Y...)	000013b0	03 00 00 00 08 90 00 00	08 10 00 00 08 00 00 00		
000013d0	93 e2 77 ca 25 8d e0 ba	6e f0 58 08 bf 09 77 8b	H..U...n..X...w...	000013c0	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00		
000013e0	e1 dd 6b 6d 77 27 1e 05	25 42 4c b5 66 95 79 b6	k.mw...*..KL..F..y...	000013d0	5b 00 00 00 0f 00 00 00	03 00 00 00 10 90 00 00	[.....	
000013f0	0a 3a 48 71 28 e1 d6 11	74 48 5e a1 f3 e4 e9 27	h.Qg...+..th...+...	000013e0	10 10 00 00 08 00 00 00	00 00 00 00 00 00 00 00		
00001400	6d 8e 44 52 e4 bb 4c 42	a5 ba 9e c7 2d 01 fe f5 ab	m.DR...+..B...+..h...	000013f0	01 00 00 00 00 00 00 00	67 00 00 00 01 00 00 00	+...g.....	
00001410	1a 17 83 0e b6 9c 17 0c	84 ad 3c 2d 03 ff 1a 82	H...&...&...&...&...&...	00001400	03 00 00 00 18 90 00 00	18 10 00 00 08 00 00 00		
00001420	ef c9 33 30 75 3b 30 33	ce bc 00 cc 0c c7 d4 dc	L..3..uq03....	00001410	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00		
00001430	d4 21 47 c5 af 03 de 0e	8a 2e 8c 91 00 7d 68 db da	L..3..uq03....	00001420	6e 00 00 00 06 00 00 00	03 00 00 00 20 90 00 00	n.....	
00001440	48 f9 9e 18 d8 e8 26 b9	f7 aa 0e 47 01 5c d2 43	H...&...&...&...&...&...	00001430	20 10 00 00 c8 00 00 00	04 00 00 00 00 00 00 00		
00001450	fd 5f 0f ca ee cc c3 df	b2 59 95 15 33 55 d0 51	W...&...&...&...&...&...	00001440	04 00 00 00 08 00 00 00	77 00 00 00 01 00 00 00		
00001460	04 b7 46 ae ef ab 9a 17	4d 79 ed 97 d5 95 1e c2	F.....J....	00001450	03 00 00 00 e8 90 00 00	e8 10 00 00 58 00 00 00		
00001470	4c 8d 7f 6c 5d 36 47	09 66 a5 ad 66 8b e1 8d	L..u..1..6...f..f...	00001460	00 00 00 00 00 00 00 00	04 00 00 00 04 00 00 00		
00001480	c2 70 23 47 03 b7 9d	92 d2 59 09 b3 c0 68 b8	p..G...+..Y...+...	00001470	7c 00 00 00 08 00 00 00	03 00 00 00 40 91 00 00	8.....	
00001490	21 60 5c 10 a9 8e 7b 0f	43 32 93 27 7f 18 82 53	f\...\C2...+..S...	00001480	40 11 00 00 10 00 00 00	00 00 00 00 00 00 00 00	8.....	

DEMO

```

00001160 8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da |...k.F+...^....| 00001150 30 00 41 28 00 00 00 61 65 61 62 69 00 01 1e 00 |0.A[...aeebi....|
00001170 5c c5 e8 1f 15 cc d2 86 78 13 07 1e 4d f4 63 c7 |...x...M.c...| 00001160 00 00 05 35 54 45 00 06 04 08 01 09 01 12 04 14 |...5TE.....|
00001180 89 61 80 06 96 46 59 d0 3c 8f ad 0c 1b aa 0e 85 |...FV.3D....| 00001170 01 15 01 17 03 18 01 19 01 1a 02 00 2e 73 68 73 |...shs.....|
00001190 61 08 a1 9e 99 5e d9 19 fc 41 ba 54 55 d5 92 8d |a...TU....| 00001180 74 72 74 61 62 00 2e 69 6e 74 65 72 70 00 2e 68 |tstab.interp.h|
000011a0 bf 2f 24 c2 b9 26 d0 02 22 9a 8e aa 76 2e 1c 8f |...$.k...v...| 00001190 61 73 68 00 2e 64 79 6e 73 79 6d 00 2e 64 79 6e |lash.dynsym.dyn|
000011b0 b4 03 1d 7d 12 3f 0f 6e 54 37 5f c6 46 76 36 cf |...7.nt7M.Kv6..| 000011a0 73 74 72 00 2e 72 65 6c 2e 70 6c 74 00 2e 74 65 |str.rel.plt.te|
000011c0 8d 45 94 e9 7c 47 be da 55 c7 63 c0 99 ce 45 77 |...G.G.U.c...Ew| 000011b0 78 74 00 2e 72 6f 64 61 74 61 00 2e 70 72 65 69 |xt..rodata.prei|
000011d0 43 38 ff 2e 50 89 c0 92 1c f2 ae af 96 44 6f |...P.....Do| 000011c0 6e 69 74 5f 61 72 72 61 79 00 2e 69 6e 69 74 5f |init.array..init|
000011e0 49 96 c2 61 66 c6 40 e8 fe 6a 44 2c 54 88 e7 d8 |...af..B...jQ.T..| 000011d0 61 72 72 61 79 00 2e 66 69 6e 69 5f 61 72 72 61 |array..fini arra|
000011f0 17 aa c1 92 7e 9b 4c f8 05 67 7e 19 53 0c 06 0f |...L.g...S...| 000011e0 79 00 2e 63 74 6f 72 73 00 2e 64 79 6e 61 6d 69 |y.ctors..dynami|
00001200 cf b4 d0 33 46 8e da 73 49 e0 05 ef 9d 9e fc 0c |...3F...el...| 000011f0 63 00 2e 67 6f 74 00 2e 62 73 73 00 2e 63 6f 6d |c..got..bss.com|
00001210 a3 93 c5 b3 38 75 96 40 22 43 7f 5c f8 da 12 b6 |...8u...C...| 00001200 6d 65 6e 74 00 2e 41 52 4d 2e 61 74 72 69 62 |ment..ARM.attrib|
00001220 de 67 3b 6b 02 b3 70 4a 90 18 04 66 03 20 01 1e |...gik...pf....| 00001210 75 74 65 73 00 00 00 00 00 00 00 00 00 00 00 |utes.....|
*
00001230 76 00 3b 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001250 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001260 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001250 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001270 f1 ec f9 9c fd eb ze a5 bb 9/ /1 99 f4 be c3 88 |.....f.q.n...| 00001260 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 |.....|
00001280 8b 3a bf 33 8e 67 ea 84 af ab f8 14 56 1d 40 82 |...3.g.....V.B..| 00001270 29 00 00 00 00 09 00 00 00 00 00 00 00 00 00 |.....|
00001290 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001280 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001290 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001310 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001320 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001310 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001330 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001320 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001340 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001330 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001350 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001340 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001360 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001350 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001370 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001360 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001380 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001370 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001390 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001380 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001390 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001410 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001420 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001410 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001430 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001420 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001440 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001430 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001450 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001440 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001460 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001450 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001470 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001460 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001480 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001470 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001490 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....| 00001480 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|

```

Unpacking

Memory Dump = Optimized DEX

► baksmali.jar : odex -> smali

► smali.jar : smali -> dex

LIAPP: Level 2



```
00001160 8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da |.kf.+.^.....| 00001150 30 00 41 28 00 00 00 61 65 61 62 69 00 01 1e 00 |0.A[...aeebi....|
00001170 5c c5 e8 1f 15 c0 d2 86 78 13 07 1e 4d f4 63 c7 |.b.....x...M.c.| 00001160 00 00 05 35 54 45 00 06 04 08 01 09 01 12 04 14 |...5TE.....|
00001180 89 61 80 06 96 46 59 d0 3c 4f ad 0c 1b aa 0e 85 |.b.....PY.30....| 00001170 01 15 01 17 03 18 01 19 01 1a 02 00 2e 73 68 73 |...shs.....|
00001190 61 08 a1 9e 99 5e 49 19 f0 81 be 54 05 92 8d |a.....TU.....| 00001180 74 72 74 61 62 00 2e 69 6e 74 65 72 70 00 2e 68 |tstab.interp.h|
000011a0 fb 2f 24 c2 b9 26 d0 02 22 9a 8e aa 76 2e 1c 8f |./$.b.....v.....| 00001190 61 73 68 00 2e 64 79 6e 73 79 69 00 2e 64 79 6e |lash.dynsym.dyn|
000011b0 b4 03 1d 78 12 3f 0f 6e 54 37 57 6c 4b 76 3e cf |.j..?..nT.W.v6..| 000011a0 73 74 72 00 2e 72 65 6c 2e 70 6c 74 00 2e 74 65 |str..rel.plt.te|
000011c0 8d 45 94 9f 7c 47 be da 55 c7 63 c0 99 ce 45 77 |.E..|G..U.c...Ew| 000011b0 78 74 00 2e 72 6f 64 61 74 61 00 2e 70 72 65 69 |xt..rodاتا.prei|
000011d0 43 38 ff 2e 50 89 c0 92 1c f2 ae af 96 44 6f |C8..P.....Do| 000011c0 6e 69 74 5f 61 72 72 61 79 00 2e 69 6e 69 74 5f |nit.array..init|
000011e0 49 96 c2 61 66 c6 40 e8 fe 6a 44 2c 54 88 e7 d8 |I..af..b...j.T...| 000011d0 61 72 72 61 79 00 2e 66 69 6e 69 5f 61 72 72 61 |array..fini arra|
000011f0 17 aa c1 92 7e 9c 4c f8 05 07 19 53 c0 06 0f |..L..g...S.....| 000011e0 79 00 2e 63 74 6f 72 73 00 2e 64 79 6e 61 6d 69 |y..ctors.dynami|
00001200 cf b4 0d 33 46 8e da 73 49 e0 05 ef 9d 9e fc 0c |..F...f.....| 000011f0 63 00 2e 67 6f 74 00 2e 62 73 73 00 2e 63 6f 6d |c...got..bss.com|
00001210 a3 93 c5 b5 38 75 96 40 22 43 7f 5c f8 da 12 b6 |..8u..C.....| 00001200 6d 65 6e 74 00 2e 41 52 4d 2e 61 74 72 72 69 62 |ment..ARM.attrib|
00001220 de 67 3b 6b 02 b3 70 4a 09 18 04 66 03 20 01 1e |.g.k..p.j.....| 00001210 75 74 65 73 00 00 00 00 00 00 00 00 00 00 00 |utes.....|
* |.....| 00001220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001240 76 29 3c 26 e6 ee 85 32 02 11 e5 a4 a4 1f 3a 78 |v(<.....2.....:x| 00001230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |*|
00001250 36 42 f1 5a 24 86 1f 9e 33 35 ff 82 b3 d6 d5 2e |68.Z$...35.....| 00001240 0b 00 00 00 01 00 00 00 02 00 00 00 d4 80 00 00 |.....|
00001260 ea b6 f6 20 c4 b2 44 8d 1f 90 c0 e4 a8 d2 2f f7 |.....D...../..| 00001250 d4 00 00 00 13 00 00 00 00 00 00 00 00 00 00 |.....|
00001270 16 89 a2 ef c5 28 70 8f 8a d6 8b 4b a8 58 ed b2 |.....8n..K..Y...| 00001260 01 00 00 00 00 00 00 00 13 00 00 00 05 00 00 |.....|
00001280 |.....| 00001270 |.....|
00001290 |.....| 00001280 |.....|
00001300 |.....| 00001290 |.....|
00001310 |.....| 00001300 |.....|
00001320 |.....| 00001310 |.....|
00001330 |.....| 00001320 |.....|
00001340 |.....| 00001330 |.....|
00001350 |.....| 00001340 |.....|
00001360 85 a7 1c 32 55 24 de d1 e2 84 cc b9 1e 7d 91 de |...ZUS.....}...| 00001350 10 00 00 00 00 00 00 00 38 00 00 00 01 00 00 00 |.....8.....|
00001370 a5 55 9f 06 0b 9a cc 8e 89 64 21 61 62 f6 d6 d6 |.U.^.....dlab...| 00001360 32 00 00 00 38 89 00 00 38 09 00 00 e0 02 00 00 |2...8...8.....|
00001380 df 6f cf 51 ee 1d 9b cb 32 15 2b d9 4d c2 53 91 |.o.Q.....2..+..B.S.| 00001370 00 00 00 00 00 00 00 00 04 00 00 00 01 00 00 00 |.....|
00001390 01 09 2a c2 9e 1e 85 93 59 ff e6 cf 18 7d 20 29 |K.....*.....Y..)| 00001380 40 00 00 00 10 00 00 00 03 00 00 00 00 90 00 00 |@.....|
000013a0 4b b6 1c d8 cb f2 7f 66 54 aa c3 84 91 af f7 95 |.K.....F.....E...| 00001390 00 10 00 00 08 00 00 00 00 00 00 00 00 00 00 |.....|
000013b0 5e f5 fa 16 f3 0e b6 9c 07 60 fd f5 6f 1f fe bc 1a fe |^.....o.n.....| 000013a0 01 00 00 00 08 00 00 00 4f 00 00 00 0e 00 00 00 |.....0.....|
000013c0 1a 17 83 0e b6 9c 15 0c 84 ad 3c 2d 03 ff 1a 82 |.....<.....<...| 000013b0 03 00 00 00 08 90 00 00 08 10 00 00 08 00 00 00 |.....|
000013d0 93 e2 77 ca 55 e0 d0 ba 6e f0 58 08 bf 09 77 8b |.w.U.....n...x..w..| 000013c0 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 |.....|
000013e0 e1 dd 6b 6d 77 27 1e 25 42 4c b5 66 95 79 b6 |.k.mw...".KL-F-y..| 000013d0 5b 00 00 00 0f 0f 00 00 03 00 00 00 10 90 00 00 |.....|
000013f0 0e 3a 48 71 28 81 d6 11 74 48 5e a1 f3 e4 e9 27 |.Hq.....tH.....| 000013e0 10 10 00 00 08 00 00 00 00 00 00 00 00 00 00 |.....|
00001400 6d 8e 44 52 e4 bb c4 42 05 ab 9e c7 68 1e f5 ab |m.DR...B.....h...| 000013f0 01 00 00 00 00 00 00 00 67 00 00 00 01 00 00 00 |.....g.....|
00001410 1a 17 83 0e b6 9c 17 0c 84 ad 3c 2d 03 ff 1a 82 |.....<.....<...| 00001400 03 00 00 00 18 90 00 00 18 10 00 00 08 00 00 00 |.....|
00001420 ff c9 33 00 75 3b 30 33 cc bc 00 cc 0c 07 d6 4c |.3..uq03.....L..| 00001410 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 |.....|
00001430 d4 21 47 c5 af 03 de e0 8a 2e 8c 91 70 c8 db da |.G.....p.....| 00001420 6e 00 00 00 06 00 00 00 03 00 00 00 20 90 00 00 |n.....|
00001440 48 f9 9e 18 d8 e8 26 b9 f7 aa 0e 47 01 5c d2 43 |H.....&.....G..<C| 00001430 20 10 00 00 c8 00 00 00 04 04 00 00 00 00 00 00 |.....|
00001450 fd 5f 0f ca ee cc c3 df b2 59 95 15 31 55 d0 51 |.W.....Y...1U.Q..| 00001440 04 00 00 08 08 00 00 00 77 00 00 00 01 00 00 00 |.....|
00001460 04 b7 46 e6 ef ab 9a 17 d4 79 ed 97 d5 95 1e c2 |.F.....f.....| 00001450 03 00 00 00 08 90 00 00 e8 10 00 00 58 00 00 00 |.....|
00001470 4c 8d 7f 6c dd 36 f7 09 66 a5 ad e6 8b e1 8d |.u..u.l.g..f..f..| 00001460 00 00 00 00 00 00 00 00 04 00 00 00 04 00 00 |.....|
00001480 c2 70 23 47 03 b7 9d 88 92 d2 59 09 b3 c0 68 b8 |.p#G.....Y...h...| 00001470 7c 00 00 00 08 00 00 00 03 00 00 00 40 91 00 00 |.....|
00001490 21 60 5c 10 a9 8e 7b f0 43 32 93 27 7f 18 82 83 |.F.....C2.....S| 00001480 40 11 00 00 10 00 00 00 00 00 00 00 00 00 00 |8.....|
```

Anti-VM

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

LIAPP: Level 2



```
00001160 8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da |.kF...+...^....| 00001150 30 00 41 28 00 00 00 61 65 61 62 69 00 01 1e 00 |0.A[...aeabi....|
00001170 5c c5 e8 1f 15 c0 d2 86 78 13 07 1e 4d f4 63 c7 |.S.....x...M.c.| 00001160 00 00 05 35 54 45 00 06 04 08 01 09 01 12 04 14 |...5TE.....|
00001180 89 61 80 06 96 46 59 d0 33 4f ad 0c 1b aa 0e 85 |.S...FY.3D.....| 00001170 01 15 01 17 03 18 01 19 01 1a 02 00 2e 73 68 73 |...shs.....|
00001190 61 08 a1 9e 99 5e d9 19 f2 81 be 54 55 d5 92 8d |a.....TU.....| 00001180 74 72 74 61 62 00 2e 69 6e 74 65 72 70 00 2e 68 |tstab.interp.h|
000011a0 fb 2f 24 c2 b9 26 d0 02 22 9a 8e aa 76 2e 1c 8f |.$.k...v.....| 00001190 61 73 68 00 2e 64 79 6e 73 79 6d 00 2e 64 79 6e |ash..dynsym..dyn|
000011b0 b4 03 1d 7d 12 3f 0f 6e 54 37 57 c6 4b 76 36 cf |.J..?.nT7M.Kv6..| 000011a0 73 74 72 00 2e 72 65 6c 2e 70 6c 74 00 2e 74 65 |str..rel.plt..te|
000011c0 8d 45 94 9e 7c 47 8b de 55 c7 63 c0 99 ce 45 77 |.E..IG..U.c...Ew| 000011b0 78 74 00 2e 72 6f 64 61 74 61 00 2e 70 72 65 69 |xt..rodata..prei|
000011d0 43 38 ff 2e 50 09 c0 92 1c f2 ae af 96 64 6f |C8..P.....Do..| 000011c0 6e 69 74 5f 61 72 72 61 79 00 2e 69 6e 69 74 5f |init.array..init_|
000011e0 49 96 c2 61 66 c6 40 e8 fe 6a 74 2c 54 88 e7 d8 |I..af.B...Q,T...| 000011d0 61 72 72 61 79 00 2e 66 69 6e 69 5f 61 72 72 61 |array..fini arra|
000011f0 17 aa c1 92 7e 9b 4c f8 05 67 7e 19 53 0c 06 0f |...L.L.g...S...| 000011e0 79 00 2e 63 74 6f 72 73 00 2e 64 79 6e 61 6d 69 |y..ctors..dynam|
00001200 cf b4 d0 33 46 8e da 73 49 e0 05 ef 9d 9e fc 0c |...3F..l.....| 000011f0 63 00 2e 67 6f 74 00 2e 62 73 73 00 2e 63 6f 6d |c..got..bss..co|
00001210 a3 93 c5 b5 38 75 96 40 22 43 7f 5c f8 da 12 b6 |...8u...C.X....| 00001200 6d 65 6e 74 00 2e 41 52 4d 2e 61 74 74 72 69 62 |ment..ARM.attrib|
00001220 de 67 3b 6b 02 b3 70 4a 90 18 04 66 03 20 01 1e |.g.k..pJ.....| 00001210 75 74 65 73 00 00 00 00 00 00 00 00 00 00 00 |utes.....|
*
00001230 b2 c3 a7 58 07 9a 9c 81 07 f9 4a b5 94 92 2b 67 |...X.....J...+g| 00001300 04 00 00 00 08 00 00 00 2d 00 00 00 01 00 00 00 |...T.....|
00001320 04 b7 46 ae ef ab 9a 17 d4 79 ed 97 d5 95 1e c2 |...F.....| 00001310 06 00 00 00 54 85 00 00 54 05 00 00 f8 00 00 00 |...T.....|
00001330
00001340
00001350
00001360
00001370
00001380
00001390
000013a0
000013b0
000013c0
000013d0
000013e0
000013f0
00001400
00001410
00001420
00001430
00001440
00001450
00001460
00001470
00001480
00001490
```

Anti-VM

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

Fix

- ▶ Run on phone and dump - **Works**

LIAPP: Level 2



```
00001160 8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da |..kF.+...^....| 00001150 30 00 41 28 00 00 00 61 65 61 62 69 00 01 1e 00 |0.A[...aeabi....|
00001170 5c c5 e8 1f 15 c0 d2 86 78 13 07 1e 4d f4 63 c7 |N.....x...M.c.| 00001160 00 00 05 35 54 45 00 06 04 08 01 09 01 12 04 14 |...5TE.....shs|
00001180 89 61 80 06 96 46 59 d0 33 4f ad 0c 1b aa 0e 85 |.S...FY.3D....| 00001170 01 15 01 17 03 18 01 19 01 1a 02 00 2e 73 68 73 |...|
00001190 61 08 a1 9e 99 5e d9 19 fc 81 be 54 55 d5 92 8d |a.....^.....TU...| 00001180 74 72 74 61 62 00 2e 69 6e 73 79 6d 72 70 00 2e 68 |ttrtab..interp..h|
000011a0 fb 2f 24 c2 b9 26 d0 02 22 9a 8e aa 76 2e 1c 8f |./$.&..."v...| 00001190 61 73 68 00 2e 64 79 6e 73 79 6d 00 2e 64 79 6e |ash..dynsym..dyn|
000011b0 b4 45 94 e9 7c 47 be da 55 c7 63 c0 99 ce 45 77 |...j.?..nT7M.Kv6..| 000011a0 73 74 72 00 2e 72 65 6c 2e 70 6c 74 00 2e 74 65 |str..rel.plt..te|
000011c0 43 38 ff 2e 50 89 c0 92 1c f2 ae af 96 44 6f |.E..[G..U.c....Ew| 000011b0 78 74 00 2e 72 6f 64 61 74 61 00 2e 70 72 65 69 |xt..rodata..prei|
000011d0 4d 45 94 e9 7c 47 be da 55 c7 63 c0 99 ce 45 77 |C8..P.....Do| 000011c0 6e 69 74 5f 61 72 72 61 79 00 2e 69 6e 69 74 5f |init_array..init_|
000011e0 49 96 c2 61 66 c6 40 e8 fe 6a 44 2c 54 88 e7 d8 |I..af..B...j0.T...| 000011d0 61 72 72 61 79 00 2e 66 69 6e 69 5f 61 72 72 61 |array..fini_arra_|
000011f0 17 aa c1 92 7e 9b 4c fe 05 67 7e 19 53 0c 06 0f |...".L..g".S...| 000011e0 79 00 2e 63 74 6f 72 73 00 2e 64 79 6e 61 6d 69 |y..ctors..dynam|
00001200 cf b4 d0 33 46 8e da 73 49 e0 05 ef 9d 9e fc 0c |...3F..eL.....| 000011f0 63 00 2e 67 6f 74 00 2e 62 73 73 00 2e 63 6f 6d |c..got..bss....t|
00001210 *
00001220 *
00001230 *
00001240 *
00001250 *
00001260 *
00001270 *
00001280 *
00001290 *
000012a0 *
000012b0 *
000012c0 *
000012d0 *
000012e0 *
000012f0 *
00001300 ef 28 b7 3c 8d c1 a0 08 b7 be 8b fd a2 86 96 73 |...<[.....v..z...| 000012f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001310 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |...<.....| 00001300 bc 04 00 00 98 00 00 00 03 00 00 00 06 00 00 00 |.....|
00001320 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |...<.....| 00001310 04 00 00 00 98 00 00 00 04 00 00 00 06 00 00 00 |.....|
00001330 *
00001340 *
00001350 *
00001360 *
00001370 *
00001380 *
00001390 *
000013a0 *
000013b0 *
000013c0 *
000013d0 *
000013e0 *
000013f0 *
00001400 6d 8e 44 52 e4 bb c4 42 a5 ba 9e c7 68 1e f5 ab |...mDr...B...h...| 000013f0 01 00 00 00 00 00 00 00 67 00 00 00 01 00 00 00 |...<...g.....|
00001410 1a 17 83 0e b6 9c 17 0c 84 ad 3c 2d 03 ff 1a 82 |...<.....<.....| 00001400 03 00 00 00 18 90 00 00 18 10 00 00 08 00 00 00 |...<.....|
00001420 ff c9 33 80 75 3b 30 33 ce bc 00 cc 0c c7 da 4c |...3..u;03....L| 00001410 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 |...<.....|
00001430 d4 21 47 c5 af 03 de e0 8a 2e 8c 91 70 d8 db da |.G.....p...| 00001420 6e 00 00 00 06 00 00 00 03 00 00 00 20 90 00 00 |n.....|
00001440 48 f9 9e 18 d8 e8 26 b9 f7 aa 0e 47 01 5c d2 43 |H.....&...G..C| 00001430 20 10 00 00 c8 00 00 00 04 00 00 00 00 00 00 00 |...<.....|
00001450 fd 57 0f ca ee c3 d3 df b2 59 95 13 55 d0 51 |.M.....Y...1U.Q| 00001440 04 00 00 08 08 00 00 00 77 00 00 00 01 00 00 00 |...<.....|
00001460 04 b7 46 ae ef ab 9a 17 d4 79 ed 97 d5 95 1e c2 |...F.....| 00001450 03 00 00 00 e8 90 00 00 e8 10 00 00 58 00 00 00 |...<.....|
00001470 4c 8d 75 fc 6c dd 36 47 d9 66 a5 ad 66 8b e1 8d |.L..u1.G..F..F..| 00001460 00 00 00 00 00 00 00 00 04 00 00 00 04 00 00 00 |...<.....|
00001480 c2 70 23 47 03 b7 9d 88 92 d2 59 09 b3 c0 68 b8 |.P.....Y...h..| 00001470 7c 00 00 00 08 00 00 00 03 00 00 00 40 91 00 00 |l.....<...B...|
00001490 21 60 5c 10 a9 8e 7b 0f 43 32 93 27 7f 18 82 83 |!\"N...{.C2....S| 00001480 40 11 00 00 10 00 00 00 00 00 00 00 00 00 00 00 |B.....|
```

Anti-VM

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

Fix

- ▶ Run on phone - **Works**
- ▶ Bypass Anti-VM

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

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



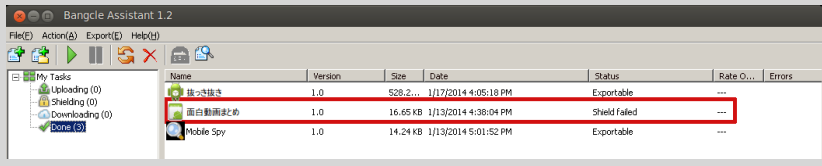
00001160	8d eb 6b 46 bf e2 2b 0e	13 f5 5e 93 85 c4 1f da	.k.f.+.^.....	00001150	30 00 41 28 00 00 00 61	65 61 62 69 00 01 1e 00	0.Aaabi....	
00001170	5c c5 e8 1f 15 cc d2 86	78 13 07 1e 4d f4 63 c7	x.....M.c.	00001160	00 00 05 35 54 45 00 06	04 08 01 09 01 12 04 14	...5fE.....	
00001180	89 61 80 06 96 46 59 0d	73 4f ad 0c 1b aa 0e 85	PY.30.....	00001170	01 15 01 17 03 18 01 19	01 1a 02 00 2e 73 68 73	shs.....	
00001190	61 08 a1 9e 99 5e d9 19	3c 81 ab 54 55 05 92 8d	TU.....	00001180	74 72 64 61 62 00 2e 69	6e 74 65 72 70 2e 2e 68	trtab..interp..h	
000011a0	bf 2f 24 c2 b9 26 0d 0f	22 9a 8e aa 76 2e 1c 8f	\$. ..v.....	00001190	61 73 68 00 2e 64 79 6e	73 79 6d 00 2e 64 79 6e	ash..dynsym..dyn	
000011b0	b4 03 1d 7d 12 3f 0f 06	54 37 5f c6 46 76 3c cf	.j..?..nTm.Kv6..	000011a0	73 74 72 00 2e 72 65 6c	2e 70 6c 74 00 2e 74 65	str..rel.plt..tel	
000011c0	8d 45 94 59 7c 47 be da	55 c7 63 c0 99 ce 45 77	.E.. G..U.c...Ew	000011b0	78 74 00 2e 72 6f 64 61	74 61 00 2e 70 72 65 69	xt..rodata..prei	
000011d0	43 38 ff 2e 50 89 c0 92	1c f2 ae af 96 44 6f 6f	C8..P.....Do	000011c0	6e 69 74 5f 61 72 72 61	79 00 2e 69 6e 69 74 5f	init.array..init_	
000011e0	49 96 c2 61 66 c6 40 e8	fe 6a 44 2c 54 88 e7 d8	.l..af...j0T...	000011d0	61 72 72 61 79 00 2e 66	69 6e 69 5f 61 72 72 61	array..fini.array_	
000011f0	17 aa c1 92 7e 9b 4c f8	05 67 19 53 c0 06 0f	L..S.....	000011e0	79 00 2e 63 74 6f 72 73	00 2e 64 79 6e 61 6d 69	.y..ctors..dynami	
00001200	cf b4 0d 33 46 8e da	73 49 e0 05 ef 9d fe c0	..3F..f.....	000011f0	63 00 2e 67 6f 74 00 2e	62 73 73 00 2e 63 6f 6d	c..got..bss.com	
00001210	a3 83 c5 35 38 75 96 f0	22 43 7f 5c 98 da 12 b6	8u..C\.....	00001200	6d 65 6e 74 00 2e 41 52	4d 2e 61 74 74 72 69 62	ment..ARM.attrib	
00001220	de 67 3b 6b 02 b3 70 4a	90 18 04 66 03 20 01 1e	.g;k..pJ.....	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	76 29 3c 26 e6 ee 85 32	02 11 e5 a4 a4 1f 3a 78	v (<.....Y.....:x	*				
00001250	36 42 1f 5a 24 86 1f 9e	33 95 cf 82 b3 d6 d5 2e	68.Z\$.....35.....	00001240	0b 00 00 00 01 00 00 00	02 00 00 00 d4 80 00 00		
00001260	ae b6 b6 20 c4 b2 44 8d	1f 30 0f 64 a8 d2 2f 7f	D...../.....	00001250	d4 00 00 00 13 00 00 00	00 00 00 00 00 00 00 00		
00001270								
00001280								
00001290								
000012a0								
000012b0								
000012c0	f1 ec f9 9c fb e6 2e a5	66 97 71 99 f4 6e c3 88	f..q..n.....	000012a0	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00		
000012e0	8b 3a bf 33 8e 67 ea 84	af ab 78 14 56 1d 40 82	...S.g...f..U..E..	000012b0	29 00 00 00 09 00 00 00	02 00 00 00 bc 84 00 00		
00001300	ef 28 b7 3c 8d c1 a0 08	b7 be 8b fd a2 86 96 73	s.....	000012f0	bc 04 00 00 98 00 00 00	03 00 00 00 06 00 00 00		
00001310	b2 c3 af 58 07 9a 9c 81	07 f9 4a b5 94 92 2b 67	X.....J.....+g	00001300	04 00 00 00 08 00 00 00	2d 00 00 00 01 00 00 00	T..T.....	
00001320	04 b7 46 ae ef ab 9a 17	4d 79 ed 97 d5 95 1e c2	F.....	00001310	06 00 00 00 54 85 00 00	54 05 00 00 f8 00 00 00		
00001330	e2 74 73 f4 0a 33 ca c5	4e 10 65 bd b2 09 df 25	S..N.e.....K	00001320	00 00 00 00 00 00 00 00	04 00 00 00 04 00 00 00		
00001340	64 1b ec dd b8 ab 1e 12	90 a3 a4 65 17 86 15 6b	J..S.....c..	00001330	32 00 00 00 01 00 00 00	06 00 00 00 50 86 00 00	2.....	
00001350	6f 59 1b 8c 47 d8 69 bb	41 48 d2 c9 b5 e3 63 6a	V..J..S..AH.....	00001340	50 06 00 00 e8 02 00 00	00 00 00 00 00 00 00 00	P.....f.....	
00001360	85 a7 1c 32 55 24 de d1	e2 84 cc b9 1e 7d 91 de	ZUS.....c.....	00001350	10 00 00 00 00 00 00 00	38 00 00 00 01 00 00 00	8.....	
00001370	ae 55 9f 9c 06 0b 9a c8	89 64 21 61 62 6e d6 d6	U..Q.....f..dab..	00001360	32 00 00 00 38 89 00 00	38 09 00 00 e0 02 00 00	2...8...8.....	
00001380	df 6f cf 51 ee 1d 9b c8	32 15 2b d9 4d c5 53 91	Q.....2..+..B..S..	00001370	00 00 00 00 00 00 00 00	04 00 00 00 01 00 00 00		
00001390	01 09 2a c2 9e 1e 85 93	99 59 e6 cf 18 7d 20 29	K.....Y.....).....	00001380	40 00 00 00 10 00 00 00	03 00 00 00 90 00 00 00	@.....	
000013a0	4b b6 1c d8 cb f2 7f 66	54 aa a3 84 91 e5 47 f9 95	K.....T.....E.....	00001390	00 10 00 00 08 00 00 00	00 00 00 00 00 00 00 00		
000013b0	5e f5 f4 f6 fc 0b d5 06	fd d5 6f 1f 16 bc 1a fe	^.....o..n.....	000013a0	01 00 00 00 00 00 00 00	4f 00 00 00 0e 00 00 00	0.....	
000013c0	1a 17 83 0e b6 9c 17 0c	84 ad 3c 2d 03 ff 1a 82	<.....<.....	000013b0	03 00 00 00 08 90 00 00	08 10 00 00 08 00 00 00		
000013d0	93 e2 77 ca 55 ed 00 ba	6e f0 58 08 bf 09 77 8b	w.U.....n..X.....w..	000013c0	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00		
000013e0	e1 dd 6b 6d 77 27 1e d5	25 42 4c b5 66 95 79 b6	k.mw...*KL..F..y..	000013d0	5b 00 00 0f 0f 00 00 00	03 00 00 00 10 90 00 00		
000013f0	0a 3a 48 71 28 81 d6 11	74 48 5e a1 f3 e4 e9 27	Hq.....tH.....	000013e0	10 10 00 00 08 00 00 00	00 00 00 00 00 00 00 00		
00001400	6d 8e 44 52 e4 bb c4 c2	a5 ba 9e c7 6d 0f 1e f5 ab	m.DR...B.....h.....	000013f0	01 00 00 00 00 00 00 00	67 00 00 00 01 00 00 00	g.....	
00001410	1a 17 83 0e b6 9c 17 0c	84 ad 3c 2d 03 ff 1a 82	<.....<.....	00001400	03 00 00 00 18 90 00 00	18 10 00 00 08 00 00 00		
00001420	ef c9 33 30 75 3b 30 33	ce bc 00 cc 0c c7 d4 dc	3..u03.....L.....	00001410	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00		
00001430	d4 21 47 c5 af 03 de 0e	8a 2e 8c 91 00 c8 db da	 G.....p.....	00001420	6e 00 00 00 06 00 00 00	03 00 00 00 20 90 00 00	n.....	
00001440	48 f9 9e 18 d8 e8 26 b9	f7 aa 9e 47 01 c5 d2 43	H.....&.....G..X..C	00001430	20 10 00 00 c8 00 00 00	04 00 00 00 00 00 00 00		
00001450	fd 5f 0f ca ee cc c3 df	b2 59 95 15 31 55 d0 51	W.....Y..10U..	00001440	04 00 00 00 08 00 00 00	77 00 00 00 01 00 00 00		
00001460	04 b7 46 ae ef ab 9a 17	4d 79 ed 97 d5 95 1e c2	F.....	00001450	03 00 00 00 e8 90 00 00	e8 10 00 00 58 00 00 00	X.....	
00001470	4c 8d 7f 6c 5d 36 47	09 66 a5 ad 66 8b e1 8d	L..u.1.6..F..f.....	00001460	00 00 00 00 00 00 00 00	04 00 00 00 04 00 00 00		
00001480	c2 70 23 47 03 b7 9d	92 d2 59 09 b3 c0 68 8b	pG.....Y.....h.....	00001470	7c 00 00 00 08 00 00 00	03 00 00 00 40 91 00 00	8.....	
00001490	21 60 5c 10 a9 8e 7b f0	43 32 93 27 7f 18 82 83	\.....C2.....S.....	00001480	40 11 00 00 10 00 00 00	00 00 00 00 00 00 00 00	8.....	

BANGCLE

Security Enforcements by bangcle.com

- ▶ Applications are scanned before packing

Rejected Application



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

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

Resistance to Dynamic Analysis

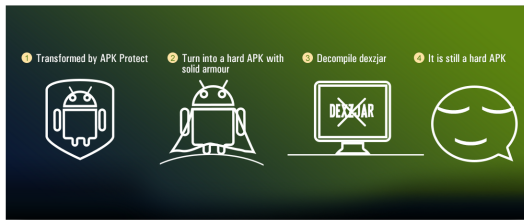
- ▶ Can't attach to main process
- ▶ Can't stack backtrace
- ▶ ptrace hooked

Memory Dump

[illegible]


```
00001160 8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da |...kF...+...^....| 00001150 30 00 41 28 00 00 00 61 65 61 62 69 00 01 1e 00 |0.A[...aeabi....|
00001170 5c c5 e8 1f 15 cc d2 86 78 13 07 1e 4d f4 63 c7 |.....x...M.c...| 00001160 00 00 05 35 54 45 00 06 04 08 01 09 01 12 04 14 |...STE.....|
00001180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001250 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001260 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001270 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001280 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001290 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001310 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001320 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001330 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001340 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001350 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001360 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001370 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001380 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001390 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001410 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001420 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001430 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001440 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001450 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001460 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001470 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001480 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001490 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
```

Source: <http://www.apkprotect.com>





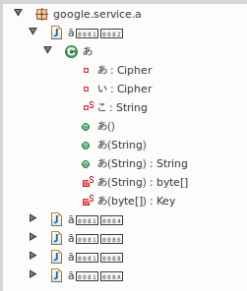
00001160	8d eb 6b 46 bf e2 2b 0e	13 f5 5e 93 85 9c 1f da	.kF.+...^....	00001150	30 00 41 28 00 00 00 61	65 61 62 69 00 01 1e 00	0.A[...aeebi....
00001170	5c c5 e8 1f 15 cc d2 86	78 13 07 1e 4d f4 63 c7	x...M.c.	00001160	00 00 05 35 54 45 00 06	04 08 01 09 01 12 04 14	...5TE.....
00001180	89 61 80 06 96 46 59 d0	33 4f ad 0c 1b aa 0e 85	.s...FY.3D....	00001170	01 15 01 17 03 18 01 19	01 1a 02 00 2e 73 68 73	...shs.....
00001190	61 08 a1 9e 99 5e d9 19	73 81 be 54 55 d5 92 8d	a...^...TU....	00001180	74 72 74 61 62 00 2e 69	6e 74 65 72 70 00 2e 68	tstab.interp.h
000011a0	fb 2f 24 c2 b9 26 0d 02	22 9a 8e aa 76 2e 1c 8f	./\$.k...v....	00001190	61 73 68 00 2e 64 79 6e	73 79 6d 00 2e 64 79 6e	ash..dynsym..dyn
000011b0	b4 03 1d 7d 12 3f 0f 6e	54 37 57 c6 46 76 3e cf	...}.?.nT7M.Kv6	000011a0	73 74 72 00 2e 72 65 6c	2e 70 6c 74 00 2e 74 65	str..rel.plt..te
000011c0	8d 45 94 e9 7c 47 be da	55 c7 63 c0 99 ce 45 77	.E.. G..U.c...Ew	000011b0	78 74 00 2e 72 6f 64 61	74 61 00 2e 70 72 65 69	xt..rodata..prei
000011d0	43 38 ff 2e 50 89 c0 92	1c f2 ae af 96 44 6f	C\$.P.....Do	000011c0	6e 69 74 5f 61 72 72 61	79 00 2e 69 6e 69 74 5f	nit.array..init_
000011e0	49 96 c2 61 66 c6 4c 0e	fe 6a 44 2c 54 88 e7 d8	.l..af..e..d,T..	000011d0	61 72 72 61 79 00 2e 66	69 6e 69 5f 61 72 72 61	array..fini arra
000011f0	17 aa c1 92 7e 9b 4c f8	05 67 7e 19 53 c0 06 0f	L.g...S..	000011e0	79 00 2e 63 74 6f 72 73	00 2e 64 79 6e 61 6d 69	y..ctors..dynam
00001200	cf b4 0d 33 46 8e da 73	49 e0 05 ef 9d fe fc 0c	...3F...f.l....	000011f0	63 00 2e 6f 6f 74 00 2e	62 73 73 00 2e 63 6f 6d	c...got..bss..co
00001210	a3 93 c5 b5 38 75 96 40	22 43 7f 5c f8 da 12 b6	...8u...C.X....	00001200	6d 65 6e 74 00 2e 41 52	4d 2e 61 74 74 72 69 62	ment..ARM.attrib
00001220	de 67 3b 6b 02 b3 70 4a	90 18 04 66 03 20 01 1e	.g;k..p.J....	00001210	75 74 65 73 00 00 00 00	00 00 00 00 00 00 00 00	utes.....
00001230	*			00001220	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001240	76 29 3c 26 e6 ee 85 32	02 11 e5 a4 a4 1f 3a 78	v(<.....2.....:x	00001230	0b 00 00 00 01 00 00 00	02 00 00 00 d4 80 00 00	
00001250	36 42 f1 5a 24 86 1f 9e	33 35 ff 82 b3 d6 d5 2e	68.7\$....35.....	00001240	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001260	*			00001250	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001270	*			00001260	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001280	*			00001270	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001290	*			00001280	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001300	*			00001290	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001310	*			00001300	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001320	*			00001310	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001330	*			00001320	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001340	*			00001330	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001350	*			00001340	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001360	*			00001350	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001370	*			00001360	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001380	*			00001370	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001390	*			00001380	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001400	*			00001390	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001410	*			00001400	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001420	*			00001410	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001430	*			00001420	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001440	*			00001430	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001450	*			00001440	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001460	*			00001450	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001470	*			00001460	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001480	*			00001470	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00001490	*			00001480	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	

Static Analysis

- ▶ apktool Fail
- ▶ dex2jar Fail
- ▶ Unzip

Static Analysis

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



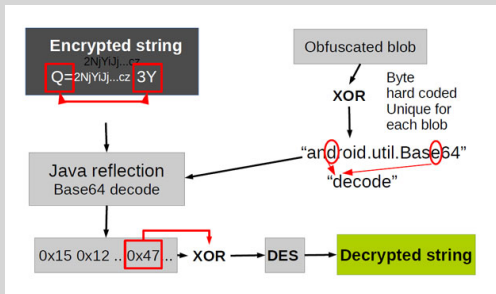
```
▼ google.service.a
  ▼ a[0001][0007]
    ▼ あ
      □ あ : Cipher
      □ い : Cipher
      □ こ : String
      ● あ()
      ● あ(String)
      ● あ(String) : String
      ■S あ(String) : byte[]
      ■S あ(byte[]) : Key
    ▶ あ[0001][0004]
    ▶ あ[0001][0005]
    ▶ あ[0001][0006]
    ▶ あ[0001][000A]
```

- ```

▼ google.service.a
 ▼ あ(0001)(0002)
 ▼ あ
 □ あ : Cipher
 □ い : Cipher
 □S こ : String
 ● あ()
 ● あ(String)
 ● あ(String) : String
 □S あ(String) : byte[]
 □S あ(byte[]) : Key
 ▶ あ(0001)(0004)
 ▶ あ(0001)(0005)
 ▶ あ(0001)(0006)
 ▶ あ(0001)(000A)

```

## String decryption



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



Props to

**Andrubis** : Analysis report reveals key

- Crypto Operations

| Timestamp          | #safeguar                           | 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 |                                     |            |           |





|          |                         |                         |                     |          |                          |                         |                       |
|----------|-------------------------|-------------------------|---------------------|----------|--------------------------|-------------------------|-----------------------|
| 00001160 | 8d eb 6b 46 bf e2 2b 0e | 13 f5 5e 93 85 9c 1f da | ..k.f+.~.~.~.~.~.   | 00001150 | 30 00 41 28 00 00 61     | 65 61 62 69 00 01 1e 00 | 0.A[...aeeabi....     |
| 00001170 | 5c c5 e8 1f 15 c0 d2 86 | 78 13 07 1e 4d f4 63 c7 | ..x..x..M.c.]       | 00001160 | 00 00 05 35 54 45 00 06  | 04 08 01 09 01 12 04 14 | ...5FE.....           |
| 00001180 | 89 61 80 06 96 46 59 0d | 33 4f ad 0c 1b aa 0e 85 | ..~.~.~.~.~.~.~.    | 00001170 | 01 15 01 17 03 18 01 19  | 01 1a 02 00 2e 73 68 73 | ...shs                |
| 00001190 | 61 08 a1 9e 99 5e d9 19 | 7c 81 ab 54 55 05 92 8d | ..a...~.~.~.~.~.    | 00001180 | 74 72 61 62 00 2e 69     | 6e 74 65 72 70 2e 2e 68 | ..trtab..interp..h    |
| 000011a0 | bf 2f 24 c2 b9 26 0d 02 | 22 9a 8e aa 76 2e 1c 8f | ..\$.~.~.~.~.~.     | 00001190 | 61 73 68 00 2e 64 79 6e  | 73 79 69 00 2e 64 79 6e | ..ash..dynsym..dyn    |
| 000011b0 | b4 03 1d 7d 12 62 3f 0f | 54 37 57 c6 46 76 3c cf | ...~.~.~.~.~.~.~.   | 000011a0 | 73 74 72 00 2e 72 65 6c  | 2e 70 6c 74 00 2e 74 65 | ..str..rel.plt..tel   |
| 000011c0 | 8d 45 94 e9 7c 47 be da | 55 c7 63 c0 99 ce 45 77 | ..E..[G..U..c..Ew   | 000011b0 | 78 74 00 2e 72 6f 64 61  | 74 61 00 2e 70 72 65 69 | ..xt..rodاتا..prei    |
| 000011d0 | 43 38 ff 2e 50 89 c0 92 | 1c f2 ae af 96 44 6f 6f | ..C.E..P.....Do     | 000011c0 | 6e 69 74 5f 6f 72 72 61  | 79 00 2e 69 6e 69 74 5f | ..init..array..init.. |
| 000011e0 | 49 96 c2 61 66 c6 4c 08 | fe 6a 44 2c 54 88 e7 d8 | ..I..af..~.~.~.~.~. | 000011d0 | 61 72 72 61 79 00 2e 66  | 69 6e 69 5f 61 72 72 61 | ..array..~.~.~.~.~.   |
| 000011f0 | 17 aa c1 92 7e 9b 4c f8 | 95 17 19 53 c0 06 0f    | ...~.~.~.~.~.~.~.   | 000011e0 | 79 00 2e 63 74 6f 72 73  | 00 2e 64 79 6e 61 6d 69 | ..y..ctors..dynami    |
| 00001200 | cf b4 0d 33 46 8e da 73 | 49 e0 05 ef 9d 9e fc 0c | ...~.~.~.~.~.~.~.   | 000011f0 | 63 00 2e 67 6f 74 00 2e  | 62 73 73 00 2e 63 6f 6d | ..c..got..bss..com    |
| 00001210 | a3 83 c5 b5 38 75 96 40 | 22 43 7f 5c f8 da 12 b6 | ...~.~.~.~.~.~.~.   | 00001200 | 6d 65 6e 74 00 2e 41 52  | 4d 2e 61 74 74 72 69 62 | ..ment..ARM.attrib    |
| 00001220 | de 67 3b 6b 02 b3 70 4a | 90 18 04 66 03 20 01 1e | ..g~k~.~.~.~.~.     | 00001210 | 75 74 65 73 00 00 00 00  | 00 00 00 00 00 00 00 00 | ..utes.....           |
| 00001230 |                         |                         |                     | 00001220 | 00 00 00 00 00 00 00 00  | 00 00 00 00 00 00 00 00 | .....                 |
| 00001240 | 76 29 3c 26 e6 ee 85 32 | 02 11 e5 a4 a4 1f 3a 78 | v)(<~.~.~.~.~.~.~.  | 00001230 | 0b 00 00 00 01 00 00 00  | 02 00 00 00 d4 80 00 00 | .....                 |
| 00001250 | 36 42 1f 5a 24 86 1f 9e | 13 35 cf 82 b3 d6 d5 2e | [68.Z\$~.~.~.~.~.   | 00001240 | 04 00 00 00 1.3 00 00 00 | 00 00 00 00 00 00 00 00 | .....                 |
| 00001260 | ae b6 f6 20 c4 b2 44 8d | 1f 90 0f 4a a8 02 2f 7f | ...~.~.~.~.~.~.~.   | 00001250 |                          |                         | .....                 |
| 00001270 |                         |                         |                     |          |                          |                         | .....                 |
| 00001280 |                         |                         |                     |          |                          |                         | .....                 |
| 00001290 |                         |                         |                     |          |                          |                         | .....                 |
| 000012a0 |                         |                         |                     |          |                          |                         | .....                 |
| 000012b0 |                         |                         |                     |          |                          |                         | .....                 |
| 000012c0 |                         |                         |                     |          |                          |                         | .....                 |
| 000012d0 | f1 ec f9 9c fb e6 2e a5 | 66 97 71 99 f4 6e c3 88 | ...f..q..n..~.      | 00001260 | 00 00 00 00 00 00 00 00  | 01 00 00 00 00 00 00 00 | .....                 |
| 000012e0 | 8b 3a bf 33 8e 67 ea 84 | af ab f8 14 56 1d 40 82 | ...~.~.~.~.~.~.~.   | 00001270 | 29 00 00 00 09 00 00 00  | 02 00 00 00 bc 84 00 00 | .....                 |
| 000012f0 | ef 28 b7 3c 8d c1 a0 08 | b7 be 8b fd a2 86 96 73 | ..~.~.~.~.~.~.~.    | 00001280 | bc 04 00 00 98 00 00 00  | 03 00 00 00 06 00 00 00 | .....                 |
| 00001300 | b2 c3 af 57 08 9a 9c 81 | 07 f9 4a b5 94 92 2b 67 | ..~.~.~.~.~.~.~.    | 00001290 | 04 00 00 00 08 00 00 00  | 2d 00 00 00 01 00 00 00 | .....                 |
| 00001310 | 04 b7 46 ae ef ab 9a 17 | 4d 79 ed 97 d5 95 1e c2 | ..~.~.~.~.~.~.~.    | 00001300 | 06 00 00 00 54 85 00 00  | 54 05 00 00 f8 00 00 00 | .....                 |
| 00001320 | e2 74 73 f4 0a 33 ca c2 | 4e 10 65 bd b2 09 df 25 | ..d...~.~.~.~.~.    | 00001310 | 00 00 00 00 00 00 00 00  | 04 00 00 00 04 00 00 00 | .....                 |
| 00001330 | 64 1b ec dd b8 ab 1e 12 | 50 a3 a4 65 17 86 15 6b | ..d...~.~.~.~.~.    | 00001320 | 32 00 00 00 01 00 00 00  | 06 00 00 00 50 86 00 00 | .....                 |
| 00001340 | 6f 59 1b 8c 47 d7 c8 69 | db 41 48 d2 c8 b3 63 6a | ..V..J..~.~.~.~.    | 00001330 | 50 06 00 00 e8 02 00 00  | 00 00 00 00 00 00 00 00 | .....                 |
| 00001350 | 85 a7 1c 32 55 24 de d1 | e2 84 cc b9 1e 7d 91 de | ..ZUS..~.~.~.~.     | 00001340 | 10 00 00 00 00 00 00 00  | 38 00 00 00 01 00 00 00 | .....                 |
| 00001360 | a5 55 9f 08 06 9a 8c 3e | 89 64 21 61 62 66 d6 d6 | ..U..~.~.~.~.~.     | 00001350 | 32 00 00 00 38 89 00 00  | 38 09 00 00 e0 02 00 00 | .....                 |
| 00001370 | df 6f cf 51 ee 1d 9b c8 | 32 15 2b d9 4d c2 53 91 | ..o..Q...~.~.~.~.   | 00001360 | 00 00 00 00 00 00 00 00  | 04 00 00 00 01 00 00 00 | .....                 |
| 00001380 | 01 09 2a c2 9e 1e 85 93 | 59 9f e6 cf 18 7d 20 29 | ..K...~.~.~.~.~.    | 00001370 | 40 00 00 00 10 00 00 00  | 03 00 00 00 00 90 00 00 | .....                 |
| 00001390 | 4b b6 1c d8 cb f2 7f 66 | 54 aa a3 84 91 a5 f7 95 | ..~.~.~.~.~.~.~.    | 00001380 | 00 10 00 00 08 00 00 00  | 00 00 00 00 00 00 00 00 | .....                 |
| 000013a0 | 1e f5 f4 f6 fc 0d 05 60 | fd d5 6f 1f fe bc 1a fe | ..~.~.~.~.~.~.~.    | 00001390 | 01 00 00 00 00 00 00 00  | 4f 00 00 00 0e 00 00 00 | .....                 |
| 000013b0 | 1a 17 83 0e b6 9c 17 0c | 84 ad 3c 2d 03 f1 82    | ...~.~.~.~.~.~.~.   | 00001400 | 03 00 00 00 08 90 00 00  | 08 10 00 00 08 00 00 00 | .....                 |
| 000013c0 | 93 e2 77 ca 55 ed d0 ba | 6e f0 58 08 bf 09 77 8b | ..W..U..~.~.~.~.    | 00001410 | 00 00 00 00 00 00 00 00  | 01 00 00 00 00 00 00 00 | .....                 |
| 000013d0 | e1 dd 6b 6d 77 27 1e d5 | 22 4b 4c b5 65 95 79 b6 | ..~.~.~.~.~.~.~.    | 00001420 | 5b 00 00 00 0f 00 00 00  | 03 00 00 00 10 90 00 00 | .....                 |
| 000013e0 | 0e 3a 48 71 28 81 d6 11 | 74 48 5e a1 f3 e4 9e 27 | ..Hq[...~.~.~.~.    | 00001430 | 10 10 00 00 08 00 00 00  | 00 00 00 00 00 00 00 00 | .....                 |
| 000013f0 | 6d 8e 44 52 e4 bb c4 c2 | a5 ba 9e c7 68 1e f5 ab | ..m..DR...~.~.~.    | 00001440 | 01 00 00 00 00 00 00 00  | 67 00 00 00 01 00 00 00 | .....                 |
| 00001400 | 1a 17 83 0e b6 9c 17 0c | 84 ad 3c 2d 03 f1 82    | ...~.~.~.~.~.~.~.   | 00001450 | 03 00 00 00 18 90 00 00  | 18 10 00 00 08 00 00 00 | .....                 |
| 00001410 | ef c9 33 30 75 3b 30 33 | ce bc 00 cc 0c 07 d4 dc | ..~.~.~.~.~.~.~.    | 00001460 | 00 00 00 00 00 00 00 00  | 01 00 00 00 00 00 00 00 | .....                 |
| 00001420 | d4 21 47 c5 af 03 de e0 | 8a 2e 8c 91 00 c8 db da | ..[G...~.~.~.~.     | 00001470 | 6e 00 00 00 06 00 00 00  | 03 00 00 00 20 90 00 00 | .....                 |
| 00001430 | 48 f9 9e 18 d8 e8 26 b9 | f7 aa 0e 47 01 5c d2 43 | ..H...~.~.~.~.~.    | 00001480 | 20 10 00 00 c8 00 00 00  | 04 00 00 00 00 00 00 00 | .....                 |
| 00001440 | fd 5f 0f ca ee cc c3 df | d2 59 95 15 31 55 d0 51 | ..~.~.~.~.~.~.~.    | 00001490 | 04 00 00 00 08 00 00 00  | 77 00 00 00 01 00 00 00 | .....                 |
| 00001450 | 04 b7 46 ae ef ab 9a 17 | 4d 79 ed 97 d5 95 1e c2 | ..~.~.~.~.~.~.~.    | 000014a0 | 03 00 00 00 e8 90 00 00  | e8 10 00 00 58 00 00 00 | .....                 |
| 00001460 | 4c 8d 75 fc 6c dd 36 47 | d9 66 a5 ad 66 8b e1 8d | ..L..u..~.~.~.~.    | 000014b0 | 00 00 00 00 00 00 00 00  | 04 00 00 00 04 00 00 00 | .....                 |
| 00001470 | c2 70 23 47 03 bf 9d    | 92 d2 59 09 b3 c0 68 b8 | ..pG...~.~.~.~.     | 000014c0 | 7c 00 00 00 08 00 00 00  | 03 00 00 00 40 91 00 00 | .....                 |
| 00001480 | 21 60 5c 10 a9 8e 7b 0f | 43 32 93 27 7f 18 82 83 | ..~.~.~.~.~.~.~.    | 000014d0 | 40 11 00 00 10 00 00 00  | 00 00 00 00 00 00 00 00 | .....                 |
| 00001490 |                         |                         |                     |          |                          |                         | .....                 |

# MALWARE AND DETECTION





# Packed malware in the wild

|          |                                                 |                   |          |                         |                         |                   |
|----------|-------------------------------------------------|-------------------|----------|-------------------------|-------------------------|-------------------|
| 00001160 | 8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da | .kf.+.^.....      | 00001150 | 30 00 41 28 00 00 00 61 | 65 61 62 69 00 01 1e 00 | 0.A[...aeabi....  |
| 00001170 | 5c c5 e8 1f 15 c0 d2 86 78 43 07 1e 4d f4 63 c7 | .b....x...M.c.    | 00001160 | 00 00 05 35 54 45 00 06 | 04 08 01 09 01 12 04 14 | ...5TE.....       |
| 00001180 | 89 61 80 06 46 59 d0 33 4f ad 0c 1b aa 0e 85    | .b...FY.3D....    | 00001170 | 01 15 01 17 03 18 01 19 | 01 1a 02 00 2e 73 68 73 | ...shs.....       |
| 00001190 | 61 08 a1 9e 99 5e d9 19 fc 81 be 54 55 d5 92 8d | a.....TU.....     | 00001180 | 74 72 74 61 62 00 2e 69 | 6e 74 65 72 70 00 2e 68 | tstab.interp.h    |
| 000011a0 | fb 2f 24 c2 9b 26 d0 02 22 9a 8e aa 76 2e 1c 8f | .\$.b...v.....    | 00001190 | 61 73 68 00 2e 64 79 6e | 73 79 6d 00 2e 64 79 6e | ash..dynsym..dyn  |
| 000011b0 | b4 03 1d 7d 12 3f 0f 6e 54 37 57 c6 4b 76 36 cf | .j..?.nT7M.Kv6.   | 000011a0 | 73 74 72 00 2e 72 65 6c | 2e 70 6c 74 00 2e 74 65 | str..rel.plt..te  |
| 000011c0 | 8d 45 94 e9 7c 47 be da 55 c7 63 c0 99 ce 45 77 | .E..[G..U.c...Ew  | 000011b0 | 78 74 00 2e 72 6f 64 61 | 74 61 00 2e 70 72 65 69 | xt..rodata..prei  |
| 000011d0 | 43 38 ff 2e 50 89 c0 92 1c f2 ae af 96 44 6f    | C8..P.....Do      | 000011c0 | 6e 69 74 5f 61 72 72 61 | 79 00 2e 69 6e 69 74 5f | init.array..init_ |
| 000011e0 | 49 96 c2 61 66 c6 40 e8 fe 6a 44 2c 54 88 e7 d8 | I..af..B...J0.T.. | 000011d0 | 61 72 72 61 79 00 2e 66 | 69 6e 69 5f 61 72 72 61 | array..finiarra   |
| 000011f0 | 17 aa c1 92 7e 9b 4c f8 05 67 7e 19 53 0c 06 0f | .....L.g...S...   | 000011e0 | 79 00 2e 63 74 6f 72 73 | 00 2e 64 79 6e 61 6d 69 | y..ctors..dynam   |
| 00001200 | cf b4 d0 33 46 8e da 73 49 e0 05 ef 9d 9e fc 0c | ...3F...l.....    | 000011f0 | 63 00 2e 67 6f 74 00 2e | 62 73 73 00 2e 63 6f 6d | c..got..bss..com  |
| 00001210 | a3 93 c5 b5 38 75 96 f0 22 43 7f 5c 93 da 12 b6 | .....8u...C...    | 00001200 | 5d 65 6e 74 00 2e 41 52 | 4d 2e 61 74 72 72 69 62 | ment..ARM.attrib  |
| 00001220 |                                                 |                   | 00001210 | 5f 3f 65 3f 65 3f 65 3f | 65 3f 65 3f 65 3f 65 3f |                   |
| 00001230 |                                                 |                   | 00001220 |                         |                         |                   |
| 00001240 |                                                 |                   | 00001230 |                         |                         |                   |
| 00001250 |                                                 |                   | 00001240 |                         |                         |                   |
| 00001260 |                                                 |                   | 00001250 |                         |                         |                   |
| 00001270 |                                                 |                   | 00001260 |                         |                         |                   |
| 00001280 |                                                 |                   | 00001270 |                         |                         |                   |
| 00001290 |                                                 |                   | 00001280 |                         |                         |                   |
| 000012a0 |                                                 |                   | 00001290 |                         |                         |                   |
| 000012b0 |                                                 |                   | 000012a0 |                         |                         |                   |
| 000012c0 |                                                 |                   | 000012b0 |                         |                         |                   |
| 000012d0 |                                                 |                   | 000012c0 |                         |                         |                   |
| 000012e0 |                                                 |                   | 000012d0 |                         |                         |                   |
| 000012f0 |                                                 |                   | 000012e0 |                         |                         |                   |
| 00001300 |                                                 |                   | 000012f0 |                         |                         |                   |
| 00001310 |                                                 |                   | 00001300 |                         |                         |                   |
| 00001320 |                                                 |                   | 00001310 |                         |                         |                   |
| 00001330 |                                                 |                   | 00001320 |                         |                         |                   |
| 00001340 |                                                 |                   | 00001330 |                         |                         |                   |
| 00001350 |                                                 |                   | 00001340 |                         |                         |                   |
| 00001360 |                                                 |                   | 00001350 |                         |                         |                   |
| 00001370 |                                                 |                   | 00001360 |                         |                         |                   |
| 00001380 |                                                 |                   | 00001370 |                         |                         |                   |
| 00001390 |                                                 |                   | 00001380 |                         |                         |                   |
| 000013a0 |                                                 |                   | 00001390 |                         |                         |                   |
| 000013b0 |                                                 |                   | 000013a0 |                         |                         |                   |
| 000013c0 |                                                 |                   | 000013b0 |                         |                         |                   |
| 000013d0 |                                                 |                   | 000013c0 |                         |                         |                   |
| 000013e0 |                                                 |                   | 000013d0 |                         |                         |                   |
| 000013f0 |                                                 |                   | 000013e0 |                         |                         |                   |
| 00001400 |                                                 |                   | 000013f0 |                         |                         |                   |
| 00001410 |                                                 |                   | 00001400 |                         |                         |                   |
| 00001420 |                                                 |                   | 00001410 |                         |                         |                   |
| 00001430 |                                                 |                   | 00001420 |                         |                         |                   |
| 00001440 |                                                 |                   | 00001430 |                         |                         |                   |
| 00001450 |                                                 |                   | 00001440 |                         |                         |                   |
| 00001460 |                                                 |                   | 00001450 |                         |                         |                   |
| 00001470 |                                                 |                   | 00001460 |                         |                         |                   |
| 00001480 |                                                 |                   | 00001470 |                         |                         |                   |
| 00001490 |                                                 |                   | 00001480 |                         |                         |                   |

## Known samples

- ▶ [Android/SmsSend.ND!tr](#) - ApkProtect'ed SMS sending malware
- ▶ [Bangale packed malware](#)
  - ▶ [Android/Feejar.B!tr](#)
  - ▶ [Android/FakeIns.D](#)
  - ▶ [Adware/Waps!Android](#) etc



# Detection

```

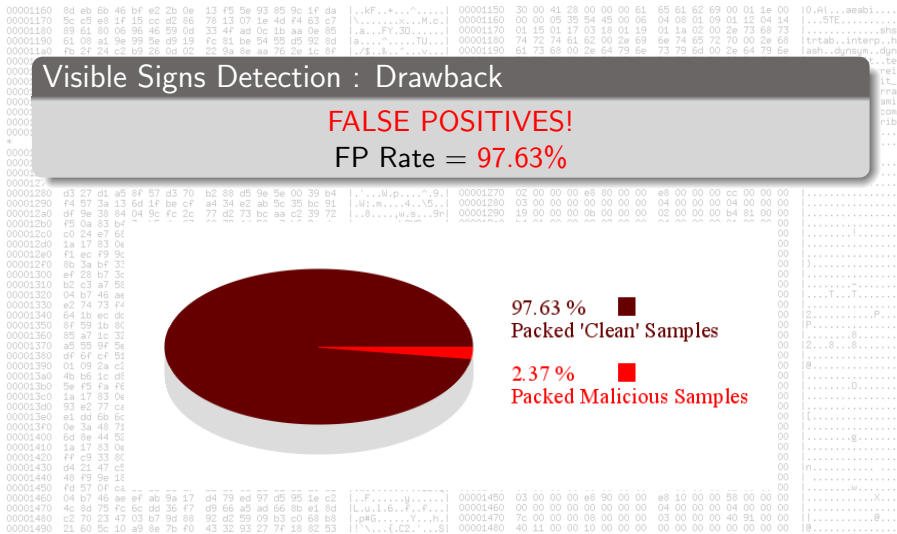
00001160 8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da |.kF.+...^....| 00001150 30 00 41 28 00 00 00 61 65 61 62 69 00 01 1e 00 |0.A[...aebi....|
00001170 5c c5 e8 1f 15 c0 d2 86 78 13 07 1e 4d f4 63 c7 | \.....x...M.c.| 00001160 00 00 05 35 54 45 00 06 04 08 01 09 01 12 04 14 |...5TE.....|
00001180 89 61 80 06 96 46 59 0d 3c 8f ad 0c 1b aa 0e 85 |.a...FY.3D....| 00001170 01 15 01 17 03 18 01 19 01 1a 02 00 2e 73 68 73 |...shs.....|
00001190 61 08 a1 9e 99 5e d9 19 fc 41 be 54 55 d5 92 8d |a.....TU....| 00001180 74 72 74 61 62 00 2e 69 6e 74 65 72 70 00 2e 68 |tntab.interp.h|
000011a0 fb 2f 24 c2 b9 26 0d 02 22 9a 8e aa 76 2e 1c 8f |./$.k...v....| 00001190 61 73 68 00 2e 64 79 6e 73 79 6d 00 2e 64 79 6e |ash.dynsym.dyn|
000011b0 b4 03 1d 7d 12 3f 0f 6e 54 37 57 c6 4b 76 36 cf |.j.j.?nT7M.Kv6| 000011a0 73 74 72 00 2e 72 65 6c 2e 70 6c 74 00 2e 74 65 |str.rel.plt.te|
000011c0 8d 45 94 e9 7c 47 8e da 55 c7 63 c0 99 ce 45 77 |.E..lG..U.c...Ew| 000011b0 78 74 00 2e 72 6f 64 61 74 61 00 2e 70 72 65 69 |xt..rodata.prei|
000011d0 43 38 ff 2e 50 8b c0 92 1c f2 ae af 96 44 6f 6f |C8..P.....Do| 000011c0 6e 69 74 5f 61 72 72 61 79 00 2e 69 6e 69 74 5f |init.array..init_|
000011e0 49 96 c2 61 66 c6 40 e8 fe 6a 44 2c 54 88 e7 d8 |l..af..B...jQ.T..| 000011d0 61 72 72 61 79 00 2e 66 69 6e 69 5f 61 72 72 61 |array..finiarra|
000011f0 17 aa c1 92 7e 9b 4c f8 05 67 7e 19 53 0c 06 0f |.....L..g...S..| 000011e0 79 00 2e 63 74 6f 72 73 00 2e 64 79 6e 61 6d 69 |y..ctors..dynami|
00001200 cf b4 0d 33 46 8e da 73 49 e0 05 ef 9d 9e fc 0c |...3F...el....| 000011f0 63 00 2e 67 6f 74 00 2e 62 73 73 00 2e 63 6f 6d |c..got..bss..com|
00001210 a3 93 c5 b5 38 75 96 40 22 43 7f 5c f3 da 12 b6 |...8u...C^X....| 00001200 6d 65 6e 74 00 2e 41 52 4d 2e 61 74 72 69 62 |ment..ARM.attrib|
00001220 de 67 3b 6b 02 b3 70 4a 90 18 04 86 03 20 01 1e |.gk..pJ.....| 00001210 75 74 65 73 00 00 00 00 00 00 00 00 00 00 00 |utes.....|
*
00001230
00001240
00001250
00001260
00001270
00001280
00001290
00001300
00001310
00001320
00001330
00001340
00001350
00001360
00001370
00001380
00001390
00001400
00001410
00001420
00001430
00001440
00001450
00001460
00001470
00001480
00001490
93 e2 77 ca 55 ed d0 ba 6e f0 58 08 bf 09 77 8b |.w.U...n.X...w.| 000013c0 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 |...|
000013a0 e1 d0 6b 6d 77 27 1e 1e 22 46 4c b5 66 95 79 b6 |.kme...KL.F-y.| 000013d0 5b 00 00 00 0f 00 00 00 03 00 00 00 10 90 00 |...|
000013b0 0e 3a 48 71 28 81 d5 11 74 48 5e a1 f3 e4 e9 27 |.Hq(...tH^...| 000013e0 10 10 00 00 08 00 00 00 00 00 00 00 00 00 00 |...|
000013c0 6d 8e 44 52 e4 bb c4 42 a5 ba 9e c7 68 1e f5 ab |m.DR...B...h...| 000013f0 01 00 00 00 00 00 00 00 67 00 00 00 01 00 00 00 |...g...|
00001410 1a 17 83 0e b6 9c 17 0c 84 ad 3c 2d 03 ff 1a 82 |.3..uq03...L..| 00001400 03 00 00 00 18 90 00 00 18 10 00 00 08 00 00 00 |...|
00001420 ff c9 33 80 75 3b 30 33 ce bc 00 cc 0c c7 da 4c |.G.....p...| 00001410 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 |...|
00001430 d4 21 47 c5 af 03 de e0 8a 2e 8c 91 70 d8 db da |.H.....&...G..C| 00001420 6e 00 00 00 06 00 00 00 03 00 00 00 20 90 00 |n...|
00001440 48 f9 9e 18 d8 ee 26 b9 f7 aa 0e 47 01 5c d2 43 |.W.....Y..U.Q| 00001430 20 10 00 00 c8 00 00 00 04 04 00 00 00 00 00 00 |...|
00001450 fd 5f 0f ca ee cc c3 df b2 59 95 15 31 55 d0 51 |.F.....| 00001440 04 00 00 00 08 00 00 00 77 00 00 00 01 00 00 00 |...|
00001460 04 b7 46 ae ef ab 9a 17 d4 79 ed 97 d5 95 1e c2 |.F.....| 00001450 03 00 00 00 e8 90 00 00 e8 10 00 00 58 00 00 00 |...|
00001470 4c 8d 75 fc 6c dd 36 47 d9 66 a5 ad 66 8b e1 8d |.u1.L.G...F...| 00001460 00 00 00 00 00 00 00 00 04 00 00 00 04 00 00 |...|
00001480 c2 70 23 47 0f b7 9d 88 92 d2 59 0b c0 c0 68 b8 |.uB.....Y...h..| 00001470 7c 00 00 00 08 00 00 00 03 00 00 00 40 91 00 00 |...|
00001490 21 60 5c 10 a9 8e 7b 0f 43 32 93 27 7f 18 82 83 | \.....C2....S| 00001480 40 11 00 00 10 00 00 00 00 00 00 00 00 00 00 |B.....|

```

## Visible Signs? Eg: Bangale

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

# Detection



# Detection



```
00001160 8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da |.k.f.+...^....| 00001150 30 00 41 28 00 00 00 61 65 61 62 69 00 01 1e 00 |0.A[...aeebi....|
00001170 5c c5 e8 1f 15 cc d2 86 78 13 07 1e 4d f4 63 c7 |\\.....x...M.c.| 00001160 00 00 05 35 54 45 00 06 04 08 01 09 01 12 04 14 |...5TE.....|
00001180 89 61 80 06 96 46 59 d9 13 4f ad 0c 1b aa 0e 85 |\\.....PY.3D....| 00001170 01 15 01 17 03 18 01 19 01 1a 02 00 2e 73 68 73 |tstab....shs|
00001190 61 08 a1 9e 99 5e d9 19 fc 81 ba 54 55 d5 92 8d |a.....TU....| 00001180 74 72 74 61 62 00 2e 69 6e 74 65 72 70 00 2e 68 |tash..interp..h|
000011a0 fb 2f 24 c2 b9 26 0d 02 22 9a 8e aa 76 2e 1c 8f |./$.&...v....| 00001190 61 73 68 00 2e 64 79 6e 73 79 6d 00 2e 64 79 6e |lash..dynsym..dyn|
000011b0 b4 03 1d 7d 18 3d 0f 06 54 37 5f aa c6 46 76 36 cf |./$.?..nT7M.Kv6.| 000011a0 73 74 72 00 2e 72 65 6c 2e 70 6c 74 00 2e 74 65 |str..rel.plt..te|
000011c0 8d 45 94 e9 7c 47 be da 55 c7 63 c0 99 ce 45 77 |.E..|G..U.c...Ew| 000011b0 78 74 00 2e 72 6f 64 61 74 61 00 2e 70 72 65 69 |xt..rodata..prei|
000011d0 43 38 ff 2e 50 8b c0 92 1c f2 ae af 96 44 6f |C8..P.....Do| 000011c0 6e 69 74 5f 61 72 72 61 79 00 2e 69 6e 69 74 5f |nit..array..init_|
000011e0 49 96 c2 61 66 c6 40 e8 fe 6a 44 2c 54 88 e7 d8 |I..af..B...Q.T..| 000011d0 61 72 72 61 79 00 2e 66 69 6e 69 5f 61 72 72 61 |array..fini..arra|
000011f0 17 aa c1 92 7e 9b 4c f8 05 67 08 19 53 0c 06 0f |.....L..B...S..| 000011e0 79 00 2e 63 74 6f 72 73 00 2e 64 79 6e 61 6d 69 |y..ctors..dynam|
00001200 cf b4 0d 33 46 8e da 73 49 e0 05 ef 9d 9e fc 0c |...3F...el....| 000011f0 63 00 2e 67 6f 74 00 2e 62 73 73 00 2e 63 6f 6d |c..got..bss..com|
00001210 a3 93 c5 b5 38 75 96 f0 22 43 7f 5c f8 da 12 b6 |...8u...C.X....| 00001200 6d 65 6e 74 00 2e 41 52 4d 2e 61 74 74 72 69 62 |ment..ARM.attrib|
00001220 de 67 3b 6b 02 b3 70 4a 90 18 04 86 03 20 01 1e |.g;k..pJ.....| 00001210 75 74 65 73 00 00 00 00 00 00 00 00 00 00 00 |utes.....|
*
00001230
00001240
00001250
00001260
00001270
00001280
00001290
00001300
00001310
00001320
00001330
00001340
00001350
00001360
00001370
00001380
00001390
00001400
00001410
00001420
00001430
00001440
00001450
00001460
00001470
00001480
00001490
```

## 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



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

## Useful Links

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

# HACKTIVITY

The End

Thank you for listening!

Contact

- Email : [rnigan\[at\]fortinet\[dot\]com](mailto:rnigan[at]fortinet[dot]com)
- Blog : [blog.fortinet.com](http://blog.fortinet.com)