

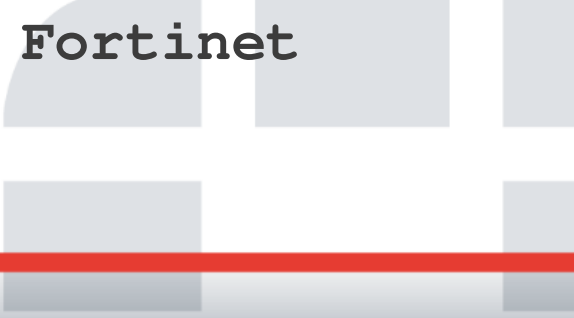
```
00001160 8d eb 6b 46 bf e2 2b 0e 13 f5 5e 93 85 9c 1f da |...kF...+...^.....| 00001150 30 00 41 28 00 00 00 61 65 61 62 69 00 01 1e 00 |0.A(...aeabi....|
00001170 5c c5 e8 1f 15 cc d2 86 78 13 07 1e 4d f4 63 c7 |\\.....x...M.c.| 00001160 00 00 05 35 54 45 00 06 04 08 01 09 01 12 04 14 |...5TE.....|
00001180 89 61 80 06 96 46 59 0d 33 4f ad 0c 1b 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 8f be 54 55 da 92 8d |a...^...TU....| 00001180 74 72 74 61 62 00 2e 69 6e 74 65 72 70 00 2e 68 |trtab..interp..hl|
000011a0 fb 2f 24 c2 b9 26 0d 02 22 9a 8e aa 76 2e 1c 8f |./$.&...".v...| 00001190 61 73 68 00 2e 64 79 6e 73 79 6d 00 2e 64 79 6e |lash..dysym..dyn|
000011b0 36 cf 45 77 |...}?.nT7W.Kv6.| 000011a0 73 74 72 00 2e 72 65 6c 2e 70 6c 74 00 2e 74 65 |str..rel.plt..te|
000011c0 44 6f e7 d8 |...E...|G...U.c...Ew| 000011b0 78 74 00 2e 72 6f 64 61 74 61 00 2e 70 72 65 69 |xt..rodata..prei|
000011e0 06 0f |C8...P.....Do| 000011c0 6e 69 74 5f 61 72 72 61 79 00 2e 69 6e 69 74 5f |nit_array..init_|
00001200 cf b4 0d 33 46 8e da 73 49 e0 05 ef 9d 9e fc 0c |I..af.@...jD,T...| 000011d0 61 72 72 61 79 00 2e 66 69 6e 69 5f 61 72 72 61 |array..fini_arra|
00001210 a3 93 c5 b5 38 75 96 f0 22 43 7f 5c f8 da 12 b6 |...^...L.g...S....| 000011e0 79 00 2e 63 74 6f 72 73 00 2e 64 79 6e 61 6d 69 |y..ctors..dynam|
00001220 de 67 3b 6b 02 b3 70 4a 90 18 04 86 03 20 01 1e |...3F...s1....| 000011f0 63 00 2e 67 6f 74 00 2e 62 73 73 00 2e 63 6f 6d |c..got..bss..com|
* 76 29 3c 26 e6 ee 85 32 02 11 e5 a4 a4 1f 3a 78 |v|&...2.....:x| * 00001240 0b 00 00 00 01 00 00 00 02 00 00 00 00 d4 80 00 00 |<.....|
00001250 36 42 f1 5a 24 86 1f 9e 33 35 ff 82 b3 d6 d5 2e |6B.Z$....35.....| 00001250 d4 00 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001260 ea b6 f6 20 c4 b2 44 8d 1f 90 c0 f4 a8 d2 2f f7 |...D...../....| 00001260 01 00 00 00 00 00 00 00 13 00 00 00 00 00 00 00 |.....|
00001270 16 89 a2 ef c5 25 70 ff 9d d6 fb 4b a9 58 c4 b2 |...%p...K.X....| 00001260 02 00 00 00 e8 80 00 00 e8 00 00 00 cc 00 00 00 |.....|
00001280 d3 27 d1 a5 8f 57 d3 70 b2 88 d5 9e 5e 00 39 b4 |...~.w.p...^..9..| 00001270 03 00 00 00 00 00 00 00 04 00 00 00 04 00 00 00 |.....|
00001290 f4 57 3a 13 6d 1f be cf a4 34 e2 ab 5c 35 bc 91 |...|l...m...4...N5..| 00001280 02 00 00 00 00 00 00 00 07 00 00 00 b4 81 00 00 |.....|
000012a0 67 9e 38 84 04 9c fc 2c 77 d2 73 23 23 b6 9a 5e |...|w...w...w...w...| 00001290 04 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 |.....|
000012b0 f5 0a 83 b4 3a b5 de 83 68 32 4d f0 23 b6 9a 5e |...|h2M...h2M...| 000012a0 02 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 |.....|
000012c0 c0 24 e7 68 23 75 83 83 1e 8a e2 5c c5 47 a5 5e |...|a#u...a#u...| 000012b0 02 00 00 00 00 00 00 00 04 00 00 00 03 00 00 00 |.....|
000012d0 1a 17 83 0e b6 9c 17 0c 86 ad 3c 2d 03 ff 1a 82 |...<-.....<-...| 000012c0 02 00 00 00 00 00 00 00 04 83 00 00 b4 03 00 00 |.....|
000012e0 f1 ec f9 9c fb 9c 2e a5 64 97 71 99 f4 6e c3 88 |...f.q...n....| 000012d0 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 f8 14 56 1d 40 82 |...3.g...V.@...| 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 08 b7 be 8b fd a2 86 96 73 |...(.X.....s| 000012f0 bc 04 00 00 98 00 00 00 03 00 00 00 06 00 00 00 |.....|
00001310 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 |.....|
00001320 04 b7 46 ae ef ab 9a 17 d4 79 ed 9f d5 95 1e c2 |...F.....y....| 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 |...ts..3..N.e...%| 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 |d.....P...e...k| 00001330 32 00 00 00 01 00 00 00 06 00 00 00 50 86 00 00 |2.....P.....|
00001350 8f 59 1b 80 4a c7 d8 69 bb 41 48 d2 e8 e3 67 8a |...Y..J...i.AH...c| 00001340 50 06 00 00 e8 02 00 00 00 00 00 00 00 00 00 00 00 |P.....|
00001360 85 a7 1c 32 55 24 de d1 e2 74 73 f4 0a 33 ca c2 |...|b...b...b...b...| 00001350 00 00 00 00 00 00 00 00 38 00 00 00 01 00 00 00 |.....8.....|
00001370 a5 55 9f 5e 0b 9a c8 3e 89 14 d1 b9 5a 7d 9b de |...|b...b...b...b...| 00001360 00 00 00 00 00 00 00 00 38 00 00 00 e0 02 00 00 |2...8...8.....|
00001380 df 6f cf 51 ee 1d 9b c8 32 15 2b 89 42 c5 53 91 |...b.Q...z...+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 f9 e6 cf 18 7d 20 29 |...*....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 45 f7 95 |...K.....T...E...| 00001390 00 10 00 00 08 00 00 00 00 00 00 00 00 00 00 00 |.....|
000013b0 5e f5 fa f6 fc db 05 60 fd d5 6f 1f 6e bc 1f bc |...|K...K...K...K...| 000013a0 01 00 00 00 00 00 00 00 4f 00 00 00 0e 00 00 00 |.....D.....|
000013c0 1a 17 83 0e b6 9c 17 0c 84 ad 3c 2d 03 ff 1a 82 |...|K...K...K...K...| 000013b0 03 00 00 00 08 00 00 00 08 10 00 00 08 00 00 00 |.....|
000013d0 93 e2 77 ca 55 ed d0 ba 6e f0 58 08 bf 09 77 8b |...k...|...K...| 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 4c b5 66 95 79 b6 |...k...|...K...| 000013d0 5f 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 |...<-.....<-...| 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 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 |.....w.....|
00001460 04 b7 46 ae ef ab 9a 17 d4 79 ed 9f d5 95 1e c2 |...F.....y....| 00001450 03 00 00 00 e8 90 00 00 e8 10 00 00 58 00 00 00 |.....X.....|
00001470 4c 8d 75 fc 6c dd 36 f7 d9 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 27 47 07 b7 0d ee 02 d2 59 0b b7 20 c8 b8 |...|...| 00001470 7c 00 00 00 08 00 00 00 03 00 00 00 40 01 00 00 |l.....a.....|
```

PUSH TO STALK

The Latest in Mobile Technologies

Ruchna NIGAM - AV Analyst/Researcher, Fortinet

European Forum AlpBach 2013



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(...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	...5TE.....
00001180	89 61 80 06 96 46 59 d0 33 4f ad 0c 1b aa 0e 85	.a...FY.30.....	00001170	01 15 01 17 03 18 01 19	01 1a 02 00 2e 73 68 73sht
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 2a 09 3b 00 62 77 93 8a aa 76 2c 00 3c 8fnT.....	00001190	71 73 68 00 2e 64 79 6e	73 79 6d 00 2e 64 79 6e	ash..dynsym..dyn
000011b0	b4 03 1c 07 3b 00 62 77 93 8a aa 76 2c 00 3c 8fnT.....	000011a0	74 72 00 2e 72 65 6c	2e 70 6c 74 00 2e 74 65	str..rel.plt..te
000011c0	8d 45 94 07 47 1b 00 62 77 93 8a aa 76 2c 00 3c 8fnT.....	000011b0	74 00 2e 72 6f 64 61	74 61 00 2e 70 72 65 69	xt..rodata..prei
000011d0	43 38 ff 50 03 62 77 93 8a aa 76 2c 00 3c 8fnT.....	000011c0	74 72 61 72 72 61	79 00 2e 69 6e 69 74 5f	nit_array..init_
000011e0	49 96 c2 61 66 0b 40 e0 fe ba 44 2c 34 88 e7 d0	..af.e..jD,	000011d0	81 72 72 81 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	...F.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..sI.....	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.\.....	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 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	00001240	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	6B.Z\$....35...	00001250	d4 00 00 00 13 00 00 00	00 00 00 00 00 00 00 00
00001260	8b b6 f6 7c c4 b2 44 d1 1f 9e 01 f8 a8 d2 2f f7D.....	00001260	01 00 00 00 00 00 00 00	00 00 00 00 05 00 00 00
00001270	03 27 d1 a5 8f 57 d3 70 b2 88 d5 9e 5e 00 39 b4W.p.....	00001270	02 00 00 00 e8 80 00 00	e8 00 00 00 cc 00 00 00
00001280	f4 57 3a 13 6d 1f be cf a4 34 e2 ab 5c 35 bc 91	.W;.m...4..\5...	00001280	03 00 00 00 00 00 00 00	04 00 00 00 04 00 00 00
00001290	df 9e 38 84 04 9c fc 2c 77 d2 73 bc aa c2 39 72	.8.....w.s...9n	00001290	19 00 00 00 0b 00 00 00	02 00 00 00 b4 81 00 00
000012a0	8b b6 f6 7c c4 b2 44 d1 1f 9e 01 f8 a8 d2 2f f7D.....	000012a0	b4 01 00 00 02 00 00 00	04 00 00 00 01 00 00 00
000012b0	1a 17 83 0e b6 9c 17 0c 84 ad 3c 2d 03 ff 1a 82<.....	000012b0	04 00 00 00 10 00 00 00	21 00 00 00 03 00 00 00
000012c0	f1 ec f9 9c fb e6 2e a5 66 97 71 99 f4 6e c3 88f.q.n.....	000012c0	02 00 00 00 b4 83 00 00	b4 03 00 00 05 01 00 00
000012d0	8b 3a bf 33 8e e7 ea 84 af ab f8 14 56 1d 40 82	...3.g.....V.e...	000012d0	29 00 00 00 09 00 00 00	02 00 00 00 bc 84 00 00
000012e0	04 b7 46 ae ef ab 9a 17 d4 79 ed 97 d5 95 1e c7	.(.<.....s.....	000012e0	bc 04 00 00 98 00 00 00	03 00 00 00 06 00 00 00
000012f0	e2 74 73 f4 0a 33 ca c2 4e 10 65 bd b2 09 df 25	...X.....J...+g	000012f0	04 00 00 00 08 00 00 00	2d 00 00 00 01 00 00 00
00001300	64 1b ec dd b8 ab 1e 12 50 a3 a4 65 17 86 15 6b	...F.....y.....	00001300	06 00 00 00 54 85 00 00	54 05 00 00 f8 00 00 00T...T.....
00001310	04 b7 46 ae ef ab 9a 17 d4 79 ed 97 d5 95 1e c7	.ts..3..N.e...%	00001310	00 00 00 00 00 00 00 00	04 00 00 00 04 00 00 00
00001320	e2 74 73 f4 0a 33 ca c2 4e 10 65 bd b2 09 df 25	d.....P..e...k	00001320	32 00 00 00 01 00 00 00	06 00 00 00 50 86 00 00	2.....P...
00001330	64 1b ec dd b8 ab 1e 12 50 a3 a4 65 17 86 15 6b	.Y..J..i.AH...c.	00001330	50 06 00 00 e8 02 00 00	00 00 00 00 00 00 00 00	P.....
00001340	04 b7 46 ae ef ab 9a 17 d4 79 ed 97 d5 95 1e c7	...2U\$....3...	00001340	10 00 00 00 00 00 00 00	38 00 00 00 01 00 00 008.....
00001350	a5 55 9f 5e 0b 9a c8 3e 89 64 21 61 62 f6 d6 d6	.U.^.....>.d!ab	00001350	32 00 00 00 38 89 00 00	38 09 00 00 e0 02 00 00	2...8...8.....
00001360	df 6f cf 51 ee 1d 9b c8 32 15 2b d9 42 c5 53 91	.o.Q.....2+.B.S.	00001360	00 00 00 00 00 00 00 00	04 00 00 00 01 00 00 00
00001370	09 2a c2 9e 1b 85 93 59 f9 e6 cf 18 7d 20 29	.*.....Y....3)	00001370	40 00 00 00 10 00 00 00	03 00 00 00 00 90 00 00	@.....
00001380	09 2a c2 9e 1b 85 93 59 f9 e6 cf 18 7d 20 29	K.....fT...E...	00001380	00 10 00 00 08 00 00 00	00 00 00 00 00 00 00 00
00001390	09 2a c2 9e 1b 85 93 59 f9 e6 cf 18 7d 20 29	^.....\o.n....	00001390	01 00 00 00 00 00 00 00	4f 00 00 00 0e 00 00 00D.....
000013a0	1a 17 83 0e b6 9c 17 0c 84 ad 3c 2d 03 ff 1a 82<.....	000013a0	03 00 00 00 08 90 00 00	08 10 00 00 08 00 00 00
000013b0	93 e2 77 ca 55 ed d0 ba 6e f0 58 08 bf 09 77 8b	...w.U...n.X...w.	000013b0	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00
000013c0	09 2a c2 9e 1b 85 93 59 f9 e6 cf 18 7d 20 29	...kwmv'."KL.f.y...	000013c0	5b 00 00 00 0f 00 00 00	03 00 00 00 00 90 00 00	[.....
000013d0	09 2a c2 9e 1b 85 93 59 f9 e6 cf 18 7d 20 29	...Hq(...tH^...3...	000013d0	10 10 00 00 08 00 00 00	00 00 00 00 00 00 00 00
000013e0	09 2a c2 9e 1b 85 93 59 f9 e6 cf 18 7d 20 29	m.DR...B...h...	000013e0	01 00 00 00 00 00 00 00	67 00 00 00 01 00 00 00g.....
000013f0	09 2a c2 9e 1b 85 93 59 f9 e6 cf 18 7d 20 29	...3.u;03.....L	000013f0	03 00 00 00 18 90 00 00	18 10 00 00 08 00 00 00
00001400	09 2a c2 9e 1b 85 93 59 f9 e6 cf 18 7d 20 29	...G.....<.....	00001400	00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00
00001410	1a 17 83 0e b6 9c 17 0c 84 ad 3c 2d 03 ff 1a 82	...w.U...n.X...w.	00001410	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00001420	09 2a c2 9e 1b 85 93 59 f9 e6 cf 18 7d 20 29	...Hq(...tH^...3...	00001420	04 00 00 00 08 00 00 00	77 00 00 00 01 00 00 00w.....
00001430	09 2a c2 9e 1b 85 93 59 f9 e6 cf 18 7d 20 29	...F.....y.....	00001430	03 00 00 00 e8 90 00 00	e8 10 00 00 58 00 00 00X...
00001440	09 2a c2 9e 1b 85 93 59 f9 e6 cf 18 7d 20 29	L.u.l.6..f..f...	00001440	00 00 00 00 00 00 00 00	04 00 00 00 04 00 00 00
00001450	09 2a c2 9e 1b 85 93 59 f9 e6 cf 18 7d 20 29	.p#G.....Y...h...	00001450	7c 00 00 00 08 00 00 00	03 00 00 00 04 91 00 00@.....
00001460	21 60 5c 10 a9 8e 7b f0 43 32 93 27 7f 18 82 53	\...{\C2.'...S	00001460	40 11 00 00 10 00 00 00	00 00 00 00 00 00 00 00	@.....
00001470						
00001480						
00001490						

→ Is Mobile Malware Really an Issue?

Evolution of Mobile Malware

→ Motivations

→ Attack Vectors

→ Rewards

→ Updates from 2013

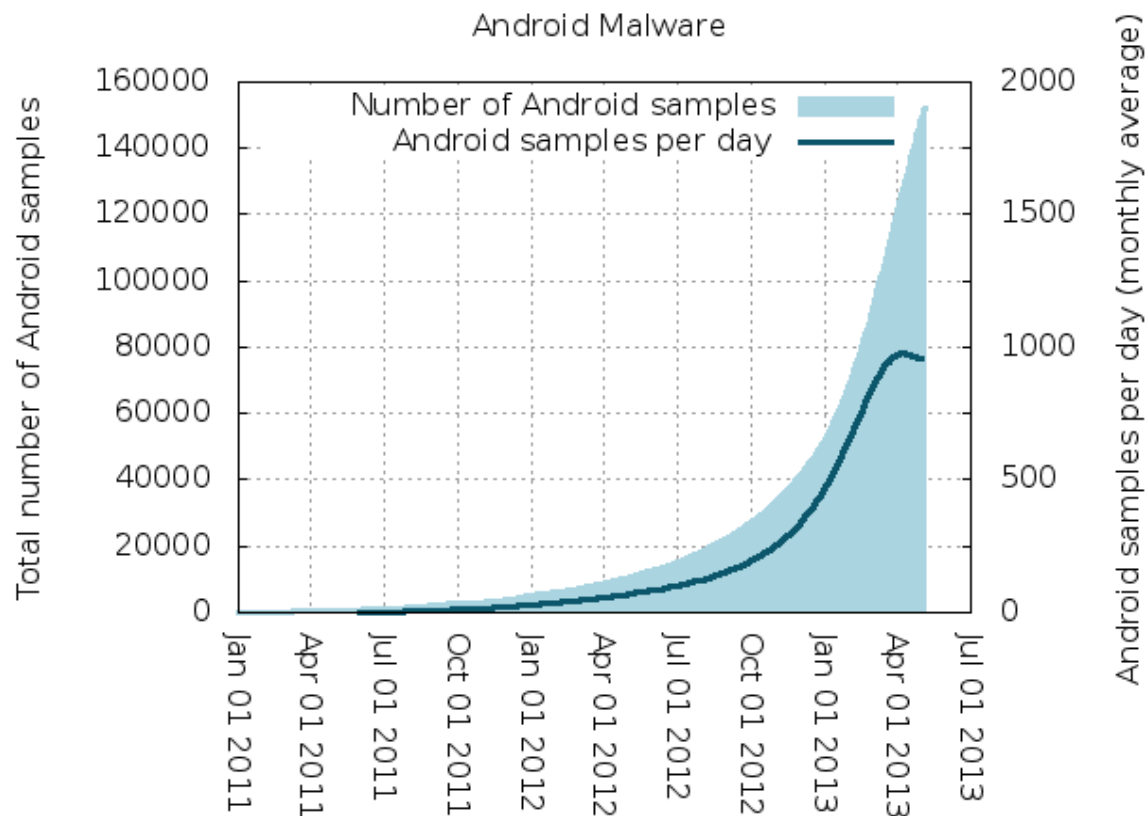
→ AndroRat Live Demo : Since Seeing is Believing

Ques: Is Mobile Malware Really an Issue?

- Answer : Yes!
- Not just an excuse to make presentations, supported with concrete statistics.
 - 15,000 signatures for mobile devices
 - ~98% of total mobile malware is for Android devices
 - Top 5 Mobile Malware on monthly Virus Watch List
<http://www.fortiguard.com/antivirus/>

Evolution of Mobile Malware

- **2004–2010:**
Symbian OS
- **2009:**
First iPhone
malware
discovered
- **Post 2010:**
Steep rise in
Android malware



Over 150,000 Android malware @ 1,000 samples per day

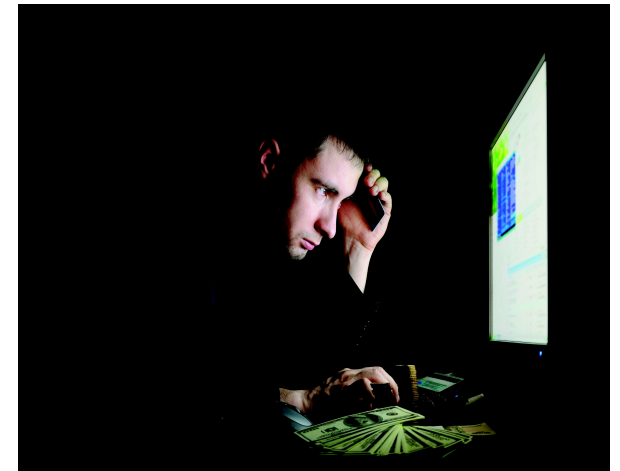
Why Android?

- **Widespread** : Windows of the mobile world
- **79% Market Share** in Q2 2013
- **Several 'App Stores'** : Possibility to bypass Android Market Verification
- **SIMPLICITY** of programming : Boon that comes at a heavy price

Motivations:

The Advantages of Attacking a Mobile Phone

- **SMARTphones** - An attacker's dream come true
 - Stays with victim at most times
 - Permanently connected to the internet (in most cases)
- **Perfect Spying Device**
 - Camera
 - Microphone
 - GPS
 - Emails
 - Social Networks
 - SMS messages



Attack Vectors:

How do I get a victim to install my application?

- **Trojans** : Nothing as it seems
 - Banking Application
 - Popular Games
 - **Fake Anti-Virus**
 - Wallpaper Applications
- **Links** on websites that download packages
Victim still needs to install
- **NEW! Targeted Attack** : Android package as attachment to an email

REWARDS !

- **MONETARY**

- **SIMPLE**

- ✓ **Premium SMS messages**

- ✓ Eg : **Android/FakeMart** - 17,000 victims in France, losses of ~500,000 euros

- **ADVANCED**

- ✓ **mTAN Stealing**

- ✓ Eg : Zitmo, Spitmo

- ✓ Used with PC malware - **Zeus, SpyEye**

- ✓ Authorize bank transfers of thousands of euros

- **DATA STEALING**

Updates from 2013

- **FEBRUARY > First PC infector : `Android/Claco.A!tr`**
- **MARCH > First Targeted Attack : `Android/Chuli.A!tr.spy`**
 - Sent to Tibetan activists as email attachment
 - Sends SMS, Contact and Location information from infected phone to the attacker
- **APRIL > `Android/BadNews.A!tr.dldr`**
 - Botnet
 - Infected around **9 million** devices
- **JULY > First Ransomware : `Android/FakeDefend.A!tr`**
 - Poses as an Anti-Virus application
 - Renders phone useless
 - Victim's Credit Card Details sent to attacker in Plain Text
 - **Fraud ransomware** - Phone not restored even after payment

AndroRat Live Demo:

Since Seeing is Believing

<http://www.youtube.com/watch?v=aVx8ntyr-yk>

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 ...5TE.....
00001180	89 61 80 06 96 46 59 0d 33 4f ad 0c 1b aa 0e 85 .a...FY.30.....	00001170	01 15 01 17 03 18 01 19 01 1a 02 00 2e 73 68 73 s
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 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 1d 7d 12 3f 0f 6e 54 37 57 c6 4b 76 36 cf ...}.?nT7W.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 nit_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_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...sI.....	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.\....	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 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	00001240	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 6B.Z\$...35.....	00001250	d4 00 00 00 13 00 00 00 00 00 00 00 00 00 00 00
00001260	ea b6 f6 20 c4 b2 44 8d 1f 90 c0 f4 a8 d2 2f f7 D...../...	00001260	01 00 00 00 00 00 00 00 13 00 00 00 05 00 00 00
00001270	16 89 a2 ef c5 25 70 ff 9d d6 fb 4b a9 58 c4 b2 %p....K.X...	00001270	02 00 00 00 e8 80 00 00 e8 00 00 00 cc 00 00 00
00001280	d3 27 d1 a5 8f 57 d3 70 b2 88 d5 9e 5e 00 39 b4 ...W.p....^9...	00001280	03 00 00 00 00 00 00 00 04 00 00 00 04 00 00 00
00001290	f4 57 3a 13 6d 1f be cf a4 34 e2 ab 5c 35 bc 91 .W;.m....4..\5..	00001290	19 00 00 00 0b 00 00 00 02 00 00 00 b4 81 00 00
000012a0	df 9e 38 84 04 9c fc 2c 77 d2 73 bc aa c2 39 72 ...8.....w.s...9r	000012a0	b4 01 00 00 00 00 00 00 04 00 00 00 01 00 00 00
000012b0	f5 0a 83 b4 3a b5 de 83 68 32 4d 50 c3 b6 6a 6e ...h?MP...	000012b0	00 00 00 00 10 00 00 00 21 00 00 00 03 00 00 00
000012c0	c0 24 e7 68 23 75 83 83 1e 8a e2 ad c5 17 6c 6a 6e ...h?MP...	000012c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000012d0	1a 17 83 0e b6 9c 17 0c 84 ad 3c 2d 03 ff 66 97 71 99 f4 6e ...h?MP...	000012d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000012e0	f1 ec f9 9c fb e6 2e a5 66 97 71 99 f4 6e 97 71 99 f4 6e ...h?MP...	000012e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000012f0	8b 3a bf 33 8e 67 ea 84 af ab f8 14 56 1d 40 82 ...3.g.....V.e...	000012f0	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...	00001300	bc 04 00 00 98 00 00 00 03 00 00 00 06 00 00 00
00001310	b2 c3 a7 58 07 9a 9c 81 07 f9 4a b5 94 92 2b 67 ...X.....J...+g	00001310	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 d4 79 ed 97 d5 95 1e c2 ...F.....y.....	00001320	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 .ts..3..N.e....%	00001330	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 d.....P...e...k	00001340	32 00 00 00 01 00 00 00 06 00 00 00 50 86 00 00 2.....P...
00001350	8f 59 1b 80 4a c7 d8 69 bb 41 48 d2 e8 e3 63 8a .Y..J..i.AH...c...	00001350	50 06 00 00 e8 02 00 00 00 00 00 00 00 00 00 00 P.....
00001360	85 a7 1c 32 55 24 de d1 e2 84 cc b9 1e 7d 91 de ...2U\$.....}...	00001360	10 00 00 00 00 00 00 00 38 00 00 00 01 00 00 00 8.....
00001370	a5 55 9f 5e 0b 9a c8 3e 89 64 21 61 62 f6 d6 d6 .U.^.....>.d!ab...	00001370	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...	00001380	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 f9 e6 cf 18 7d 20 29 ...*.....Y.....})	00001390	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 45 f7 95 K.....fT...E...	000013a0	00 10 00 00 08 00 00 00 00 00 00 00 00 00 00 00
000013b0	5e f5 fa f6 fc db 05 60 fd d5 6f 1f 0e bc 1a fe ^.....\..o.n...	000013b0	01 00 00 00 00 00 00 00 4f 00 00 00 0e 00 00 00 D.....
000013c0	1a 17 83 0e b6 9c 17 0c 84 ad 3c 2d 03 ff 1a 82 <.....	000013c0	03 00 00 00 08 90 00 00 08 10 00 00 08 00 00 00
000013d0	93 e2 77 ca 55 ed 0d ba 6e f0 58 08 bf 09 77 8b ...w.U...n.X...w...	000013d0	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 4c b5 66 95 79 b6 ...kmw'.."KL.f.y...	000013e0	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^...	000013f0	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...	00001400	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 <.....	00001410	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 c2 0c 0c c7 da 4c ...3.u;03.....L	00001420	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 .l.G.....p...	00001430	6e 00 00 00 06 00 00 00 03 00 00 00 20 90 00 00 n.....
00001440	4d f9 9e 18 d8 e8 26 b9 f7 aa 0e 47 01 5c d2 43 H.....&.....G.\.C	00001440	20 10 00 00 c8 00 00 00 04 00 00 00 00 00 00 00
00001450	fb 57 0f ca ee cc c3 df b2 59 95 15 31 55 d0 51 .W.....Y...1U.Q	00001450	04 00 00 00 08 00 00 00 77 00 00 00 01 00 00 00 w.....
00001460	04 b7 46 ae ef ab 9a 17 d4 79 ed 97 d5 95 1e c2 ...F.....y.....	00001460	03 00 00 00 e8 90 00 00 e8 10 00 00 58 00 00 00 X...
00001470	4c 8d 75 fc 6c dd 36 f7 d9 66 a5 ad 66 8b e1 8d L.u.l.6..f..f...	00001470	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 d2 a2 59 09 b3 c0 68 b8 .p#G.....Y...h...	00001480	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 53 \...{\.C2.'...S	00001490	40 11 00 00 10 00 00 00 00 00 00 00 00 00 00 00 @.....

Questions?

```
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 |...5TE.....|
00001180 89 61 80 06 96 46 59 0d 33 4f ad 0c 1b aa 0e 85 |.a...FY.30.....| 00001170 01 15 01 17 03 18 01 19 01 1a 02 00 2e 73 68 73 |.....s|
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 0d 02 22 9a 8e aa 76 2e 1c 8f |./$.&..."v...| 00001190 61 73 68 00 2e 64 79 6e 73 79 6d 00 2e 64 79 6e |ash..dynsym..dyn|
000011b0 b4 03 1d 7d 12 3f 0f 6e 54 37 57 c6 4b 76 36 cf |...}.?..nT7W.Kv6.| 000011a0 73 74 72 00 2e 72 65 6c 2e 70 6c 74 00 2e 74 65 |str..rel.plt..te|
000011c0 8d 45 94 e9 7c 47 be da 55 c7 63 c0 99 ce 45 77 |.E..|G..U.c...Ew| 000011b0 78 74 00 2e 72 6f 64 61 74 61 00 2e 70 72 65 69 |xt..rodata..prei|
000011d0 43 38 ff 2e 50 89 c0 92 1c f2 ae af af 96 44 6f |C8..P.....Do| 000011c0 6e 69 74 5f 61 72 72 61 79 00 2e 69 6e 69 74 5f |nit_array..init_|
000011e0 49 96 c2 61 66 c6 40 e8 fe 6a 44 2c 54 88 88 88 |.T..af..@..jD..T...| 000011d0 61 72 72 61 79 00 2e 66 69 6e 69 5f 61 72 72 61 |array..fini_arra|
000011f0 17 aa c1 92 7e 9b 4c f8 05 67 7e 19 53 0c 0f 0f |.....P.....S...| 000011e0 74 74 5f 72 73 00 2e 64 79 6e 61 6d 69 |y..ctors..dynam|
00001200 cf b4 0d 33 46 8e da 73 49 e0 05 ef 9d 9e f0 0c 0c |.....s.....| 000011f0 6d 6d 6d 6d 6d 6d 6d 6d 62 73 73 00 2e 63 6f 6d |c..got..bss..com|
00001210 a3 93 c5 b5 38 75 96 f0 22 43 7f 5c f8 da 06 06 |.....| 00001200 6d 6d 6d 6d 6d 6d 6d 6d 41 52 4d 2e 61 74 74 72 69 62 |ment..ARM.attrib|
00001220 de 67 3b 6b 02 b3 70 4a 90 18 04 86 03 20 01 1e |;g;k..pJ.....| 00001210 75 74 65 73 00 00 00 00 00 00 00 00 00 00 00 00 |utes.....|
* 00001240 76 29 3c 26 e6 ee 85 32 02 11 e5 a4 a4 1f 3a 78 |v)<&...2.....:x| 00001220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00001250 36 42 f1 5a 24 86 1f 9e 33 35 ff 82 b3 d6 d5 2e |6B.Z$.>...35.....| 00001240 0b 00 00 00 01 00 00 00 02 00 00 00 00 d4 80 00 00 |.....|
00001260 ea 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 9d d6 fb 4b a9 58 c4 b2 |.....%p....K.X...| 00001260 01 00 00 00 00 00 00 00 13 00 00 00 05 00 00 00 |.....|
00001280 d3 27 d1 a5 8f 57 d3 70 b2 88 d5 9e 5e 00 39 b4 |.....W.p....^..9...| 00001270 02 00 00 00 e8 80 00 00 e8 00 00 00 cc 00 00 00 |.....|
00001290 f4 57 3a 13 6d 1f be cf a4 34 e2 ab 5c 35 bc 91 |.W;.m....4..5...| 00001280 03 00 00 00 00 00 00 00 04 00 00 00 04 00 00 00 |.....|
000012a0 df 9e 38 84 04 9c fc 2c 77 d2 73 bc aa c2 39 72 |...8.....w.s...9r| 00001290 19 00 00 00 0b 00 00 00 02 00 00 00 b4 81 00 00 |.....|
000012b0 f5 0a 83 b4 3a b5 de 83 68 32 4d 50 c3 b6 9a de |.....h2MP.....| 000012a0 b4 01 00 00 02 00 00 00 04 00 00 00 01 00 00 00 |.....|
000012c0 c0 24 e7 68 23 75 83 83 1e 8a e2 ad c5 17 ac 56 |.$.h#u.....V...| 000012b0 04 00 00 00 10 00 00 00 21 00 00 00 03 00 00 00 |.....!.....|
000012d0 1a 17 83 0e b6 9c 17 0c 84 ad 3c 2d 03 ff 1a 82 |.....<.....| 000012c0 02 00 00 00 b4 83 00 00 b4 03 00 00 05 01 00 00 |.....|
000012e0 f1 ec f9 9c fb e6 2e a5 66 97 71 99 f4 6e c3 88 |.....f.q.n.....| 000012d0 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 |.....|
000012f0 8b 3a bf 33 8e 67 ea 84 af ab f8 14 56 1d 40 82 |...:3.g.....V...| 000012e0 29 00 00 00 09 00 00 00 02 00 00 00 bc 84 00 00 |.....).....|
00001300 ef 28 b7 3c 8d c1 a0 08 b7 be 8b fd a2 86 96 73 |.(<.....g.....nc| 000012f0 04 00 00 98 00 00 03 00 00 00 06 00 00 00 |.....|
00001310 b2 c3 a7 58 07 9a 9c 81 07 f9 4a b5 94 92 2b 67 |.....X.....| 00001300 00 00 00 00 00 00 00 00 2d 00 00 00 01 00 00 00 |.....-.....|
00001320 04 b7 46 ae ef ab 9a 17 d4 79 ed 97 d5 95 1e c2 |...F.....y.....| 00001310 06 00 00 00 54 85 00 00 54 05 00 00 f8 00 00 00 |.....T...T.....|
00001330 e2 74 73 f4 0a 33 ca c2 4e 10 65 bd b2 09 df 25 |.ts..3..N.e....%| 00001320 00 00 00 00 00 00 00 00 04 00 00 00 04 00 00 00 |.....|
00001340 64 1b ec dd b8 ab 1e 12 50 a3 a4 65 17 86 15 6b |d.....P..e...k...| 00001330 32 00 00 00 e1 00 00 00 06 00 00 00 50 86 00 00 |Z.....P...|
00001350 8f 59 1b 80 4a c7 d8 69 bb 41 48 d2 e8 e3 63 8a |.Y..J..i.AH...c...| 00001340 50 06 00 00 08 02 00 00 00 00 00 00 00 00 00 00 |P.....|
00001360 85 a7 1c 32 55 24 de d1 e2 84 cc b9 1e 7d 91 de |...2U$.>...3...| 00001350 10 00 00 00 00 00 00 00 38 00 00 00 01 00 00 00 |.....8.....|
00001370 a5 55 9f 5e 0b 9a c8 3e 89 64 2e 65 7d 2e 01 |.L.....>d...| 00001360 78 78 78 78 78 78 78 78 39 09 00 00 e0 02 00 00 |Z...8...8...|
00001380 df 6f cf 51 ee 1d 9b c8 32 15 20 05 11 25 01 01 |c.....g..4..| 00001370 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 |.....|
00001390 01 09 2a c2 9e 1e 85 93 59 f9 e6 cf 18 7d 20 29 |...*.....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 45 f7 95 |K.....fT...E...| 00001390 00 10 00 00 08 00 00 00 00 00 00 00 00 00 00 00 |.....|
000013b0 5e f5 fa f6 fc db 05 60 fd d5 6f 1f 06 bc 1a fe |^.....^..o.n...| 000013a0 01 00 00 00 00 00 00 00 4f 00 00 00 0e 00 00 00 |.....D.....|
000013c0 1a 17 83 0e b6 9c 17 0c 84 ad 3c 2d 03 ff 1a 82 |.....w.....X..w...| 000013b0 03 00 00 00 08 90 00 00 08 10 00 00 08 00 00 00 |.....|
000013d0 93 e2 77 ca 55 ed 0b ba 6e f0 58 08 bf 08 77 8b |...w.....X.....| 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 4c 1d 66 5b 79 8c |.j.....K.L...| 000013d0 00 00 00 00 00 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 6d 27 |.Hq(...TR...| 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 |.....<.....| 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 c2 0c 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 4d f9 9e 18 d8 e8 26 b9 f7 aa 0e 01 5c 22 43 |.....&.....| 00001430 2e 10 00 00 c8 89 00 00 04 00 00 00 00 00 00 00 |.....|
00001450 f8 57 0f ca ee cc c3 df b2 59 95 71 65 60 01 |.....Y.....| 00001440 05 00 00 00 08 00 00 00 00 00 00 01 00 00 00 |.....w.....|
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 |.....X...|
00001470 4c 8d 75 fc 6c dd 36 f7 d9 66 a5 ad 66 8b e1 8d |L.u.l.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 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 53 ||\...{.C2..'S| 00001480 40 11 00 00 10 00 00 00 00 00 00 00 00 00 00 00 |@.....|
```

Thank you!

Contact:

rnigam[at]fortinet[dot]com

http://blog.fortinet.com

Twitter: @FortiGuardLabs