Appendix – Indicators of Compromise

MD5

Android

0BC28AC5F2CADD524E7F443E06AD2A2B
39FCA709B416D8DA592DE3A3F714DCE8
70A937B2504B3AD6C623581424C7E53D
C091489A82263899D02B363B289A37F6
E12B9AF5DF1C638EF5A099961FFBE344
708445B8D358C254E861EFFFFD4F819B
3F0E8A3AD9FAB04377B8E9A57A26F972
D574D0049F797611589803643A8AA3C3
6414F4BFBDD08D70C40B107E86276DBB
90F26ADB324A8B36D2CAFDD755AA1E61
A2A8E8AC6F5FA5801395252E11AFB356
CE241B48377CA216D8F2017991C1CEF0
0BE2B5394DAFB76EFC54BD6113AC8689
D99A3C4348C88CDFA59E90D1B3B94FC3
A287A434A0D40833D3EBF5808950B858

Android payloads

MD5	Name
6964866106C0A353A7B91B580933C5D6	update_reb.zip
7E6CB66A3623258444639D1FC2FD533F	update_set.zip
D9C7349E807E0F12EAA67B2DE522954F	update_set.zip
2C21F61A8DF19D07FD0F42B631151517	update_dev.zip
4F76BDFC40529984BF8E8A05D665CEF8	parser.apk
E2D6F1263000086E3146D5B5A3B78038	startup.arm64-v8a.zip startup.armeabi.zip startup.armeabi-v7a.zip

Windows

55FB01048B6287EADCBD9A0F86D21ADF
F673BB1D519138CED7659484C0B66C5B
D3BAA45ED342FBC5A56D974D36D5F73F
395F9F87DF728134B5E3C1CA4D48E9FA
16311B16FD48C1C87C6476A455093E7A
6BCC3559D7405F25EA403317353D905F

Domains related to distribution campaign

119.network
119.business
timbox.info
vodafoneinfinity.sytes.net
vodafone.press
voda.mobi
190.network
tre.support
h3g.mobi
h3g.co
h3g.info
155wind.mobi
wind.support
windupdate.serveftp.com
skygofree.sytes.net
digimobil.mobi
kenamobile.mobi
lycamobile.mobi
postemobile.help

Command and control servers

C2 server	**Platform**
217.194.13[.]133	Android
url[.]plus	Android
negg.ddns[.]net	Android

negg1.ddns[.]net	Android
negg2.ddns[.]net	Android
79.3.197[.]89	Android
54.67.109[.]199	Android, Windows
80.21.172[.]8	Windows

Mutexes

Module	**Mutex**
system.exe	mutex_var_AU
update.exe	mutex_var_K mutex_var_xboz
network.exe	mutex_var_SE
wow.exe	mutex_var_scren
msconf.exe	mutex_var_Re_v_5

Appendix - Protocol commands of the Android implant

Command	**Short description**
install_apk	Install apk from specified URL as a fake update
mobileconn	Set mobile data enabled (3G)
resetstats	Reset internal traffic statistic
resettoken	Reset registration on c2 server
attiva	Activate FirebaseMessaging protocol
managedoc	Upload files from sdcard to c2 server
send_intent	Send specified intent[1]
wifi	Set new specified wi-fi network connection and enable it
xmpp	Connect to XMPP server
resetgw	Set a new c2 server address

[1] https://developer.android.com/reference/android/content/Intent.html

reverse	Activate reverse shell module
enable_location	Spoof request to the user to enable Google Location services
resetalarm	Restart AndroidAlarmManager service
clipboard	Enable clipboard stealing feature
camera	Record video/capture the photo after next unlocking
cancan	Upload installed applications list
filelists	Upload file structure of the memory card
runweb	Activate entry point with services
social	Steal specified app database
status	Report implant status info
accessibility	Spoof request to the user to enable accessibility service
calendar	Upload calendar events by specified period
disattiva	Stop all implant's services
registro_chiamate	Upload call logs
getfile	Upload specified file
sms	Upload stored sms
info	Upload device info (os details, remaining space etc)
stop	Stop audio recording
admin	Spoof request to the user to enable device admin
gps_n	Stop gps tracking
gps_y	Start gps tracking
net_n	Stop location tracking via Google Location services
net_y	Start location tracking via Google Location services
start	Start audio recording
location_force	Track location with high accuracy and with movement detector
cella_start	Start GSM CELL tracking
notification	Spoof request to the user to get notification listener rights
history	Steal browser history
gps_y_move	Enable gps+move detection
socialrt	Download and execute Social payload
whatsapp_msg	Steal Whatsapp message database from memory card
blacklist	Add entry to app blacklist (feature is not fully implemented)
wifi3gsetting	Use wifi or 3g to data transfer

call_recording_n	Disable calls recording feature
call_recording_y	Enable calls recording feature
rubrica	Steal contacts
geofence	Add/remove location where audio recording will turns on
cella_stop	Stop GSM CELL tracking

Appendix - Device models targeted by the exploit module

Model	**Build id**
201K	117.1.1c00
202K	101.0.2c10
ALCATEL ONE TOUCH 6030X	Jelly Bean
ASUS Pad TF300T	JRO03C.JP_epad-10.4.2.20-20121228
C1505	11.3.A.0.47
C1505	11.3.A.2.13
C2104	15.0.A.1.31
C2104	15.0.A.1.36
C2105	15.0.A.1.31
C2105	15.0.A.1.36
C5302	12.0.A.1.211
C5302	12.0.A.1.257
C5302	12.0.A.1.284
C5303	12.0.A.1.211
C5303	12.0.A.1.257
C5303	12.0.A.1.284
C5306	12.0.A.1.211
C5306	12.0.A.1.257
C5306	12.0.A.1.284
C5502	10.1.1.A.1.310

C5503	10.1.1.A.1.310
C6502	10.3.A.0.423
C6503	10.3.A.0.423
C6506	10.3.A.0.423
C6602	10.1.1.A.1.253
C6602	10.1.1.A.1.307
C6602	10.3.A.0.423
C6603	10.1.1.A.1.253
C6603	10.1.1.A.1.307
C6603	10.3.A.0.423
C6606	10.1.1.B.0.166
C6616	10.1.1.A.1.319
Dynamic_Maxi	Dynamic_Maxi
F-02E	V16R46A
F-02E	V17R48A
F-02E	V19R50D
F-03D	V24R33Cc
F-04E	V08R39A
F-05D	V08R31C
F-05D	V11R40A
F-06E	V21R48D
F-07E	V19R38A
F-07E	V20R39D
F-07E	V21R40B
F-10D	V10R42A
F-10D	V21R48A
F-10D	V22R49C
F-11D	V21R36A
F-11D	V24R40A
F-11D	V26R42B
F-12C	V21
FJL21	V23R39X
FJL21	V37R47A

FJL21	V39R48C
GT-I8190	JZO54K.I8190XXAME1
GT-I9195	JDQ39.I9195XXUAMF5
Galaxy Nexus	JOP40C
Galaxy Nexus	JZO54K
HTC6600LVW	JSS15J
HTL21	JRO03C
HTL21	JRO03C
HTL21	JRO03C
HTL21	JRO03C
HTL22	JDQ39
HTL22	JDQ39
HTL22	JZO54K
HTL22	JZO54K
HTX21	JRO03C
HTX21	JRO03C
HUAWEI G610-U20	G610-U20 V100R001C00B126
HUAWEI Y330-U01	Y330-U01 V100R001C00B133
IS11N	GRJ90
IS12S	6.1.D.1.103
IS12S	6.1.D.1.91
IS15SH	01.00.04
IS17SH	01.00.03
IS17SH	01.00.04
ISW11F	FIK700
ISW11F	FIK700
ISW11K	145.0.0002
ISW13F	V69R51I
ISW13F	V75R58A
ISW13HT	IMM76D
L-01D	IMM76D
L-01D	IMM76D
L-01D	IMM76D

L-01E	IMM76L
L-01E	JZO54K
L-01F	JDQ39B
L-01F	JDQ39B
L-02E	IMM76L
L-02E	IMM76L
L-02E	JZO54K
L-05D	JZO54K
L-06D	IMM76D
L-06D	IMM76D
L-06D	IMM76D
LG-E975	JZO54K
LGL22	JDQ39B
LGL22	JDQ39B
LGL22	KOT49I
LGL23	JDQ39B
LT22i	6.2.A.1.100
LT25i	9.1.A.1.140
LT25i	9.1.A.1.142
LT25i	9.1.A.1.145
LT26i	6.2.B.0.200
LT26i	6.2.B.0.211
LT26i	6.2.B.1.96
LT26ii	6.2.B.0.200
LT26ii	6.2.B.0.211
LT26w	6.2.B.0.200
LT26w	6.2.B.0.211
LT28h	6.2.B.0.211
LT28i	6.2.B.0.211
LT29i	9.1.B.0.411
LT29i	9.1.B.1.67
LT30p	9.1.A.1.141
LT30p	9.1.A.1.142

LT30p	9.1.A.1.145
M35h	12.0.A.1.257
M36h	10.1.1.A.1.310
N-02E	A3002501
N-02E	A3002601
N-02E	A5000331
N-02E	A5002501
N-02E	A5002601
N-03E	A7000241
N-03E	A7001821
N-03E	A7002001
N-03E	A7202001
N-03E	A7202201
N05E	A1000311
NEC-101T	112.55.12.2.02.01
Nexus 4	JDQ39
Nexus 5	KTU84P
P-02E	10.0657
P-02E	10.0659
P-02E	10.0691
P-02E	10.0733
P-02E	10.0767
P-02E	10.0798
P-02E	10.0818
P-03E	10.101
SBM203SH	S0024
SC-01E	IMM76D.SC01EOMALJ3
SC-01E	IMM76D.SC01EOMAMF2
SC-04E	JDQ39.SC04EOMUAMDI
SC-04E	JDQ39.SC04EOMUAMF1
SC-04E	JDQ39.SC04EOMUAMF2
SC-04E	JDQ39.SC04EOMUAMG2
SC-05D	IMM76D.OMLPL

SCH-I545	JDQ39.I545VRUAME7
SCL21	IMM76D.SCL21KDALJD
SGP311	10.1.C.0.370
SGP312	10.1.C.0.370
SGP321	10.1.1.A.1.307
SH-01E	02.00.02
SH-02E	02.00.02
SH-02E	02.00.03
SH-04E	01.00.02
SH-04E	01.00.03
SH-04E	01.00.04
SH-05E	01.00.05
SH-05E	01.00.06
SH-06E	01.00.01
SH-06E	01.00.05
SH-06E	01.00.06
SH-06E	01.00.07
SH-07E	01.00.03
SH-09D	02.00.03
SHL21	01.00.09
SHL21	01.01.02
SO-01E	9.1.C.0.473
SO-01E	9.1.C.1.103
SO-02E	10.1.D.0.343
SO-03E	10.1.E.0.265
SO-03E	10.1.E.0.269
SO-04D	7.0.D.1.137
SO-04D	9.1.C.0.475
SO-04D	9.1.C.1.103
SO-04E	10.1.1.D.0.179
SO-04E	10.1.1.D.2.26
SO-05D	7.0.D.1.117
SO-05D	7.0.D.1.137

SO-05D	9.1.C.0.475
SO-05D	9.1.C.1.103
SOL21	9.0.F.0.226
SOL21	9.1.D.0.395
SOL21	9.1.D.0.401
SOL22	10.2.F.3.43
SOL22	10.2.F.3.81
ST23i	11.0.A.5.5
ST23i	11.0.A.5.8
ST26a	11.2.A.0.21
ST26a	11.2.A.0.31
ST26i	11.2.A.0.21
ST26i	11.2.A.0.31
ST27a	6.2.A.1.100
ST27i	6.2.A.1.100
Sony Tablet P	TISU0144
Sony Tablet S	TISU0143
T-02D	V10R36A
URBANO PROGRESSO	010.0.3000
URBANO PROGRESSO	011.0.3100