ID: 764028
Sample Name: Cliente m#U00f3vil @firma 1.7.2 1.7.2.apk
Cookbook: defaultandroidfilecookbook.jbs
Time: 10:30:52
Date: 09/12/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

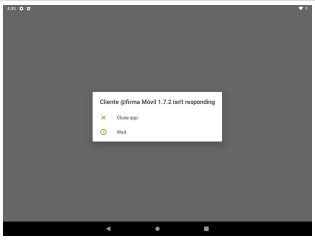
Android Analysis Report

Cliente m#U00f3vil @firma 1.7.2 1.7.2.apk

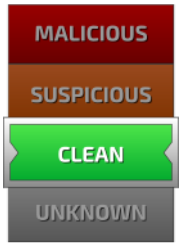
Overview

General Information

Sample Name:	Cliente m#U00f3vil @firma 1.7.2 1.7.2.apk
Analysis ID:	764028
MD5:	5a9163b46f5c74..
SHA1:	595d00ab197ef3..
SHA256:	2b4f1d122c8171..
Infos:	



Detection

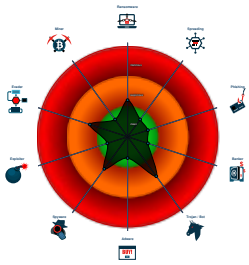


Score:	8
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Opens an internet connection
- May access the Android keyguard (…
- Lists and deletes files in the same c…
- Detected TCP or UDP traffic on non…
- Has functionality to send UDP pack…
- Installs a new wake lock (to get acti…
- Checks an internet connection is av…
- Accesses android OS build fields
- Executes native commands
- Installs an application shortcut on th…
- Performs DNS lookups (Java API)
- Requests potentially dangerous perm…

Classification



Yara Signatures

No yara matches

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

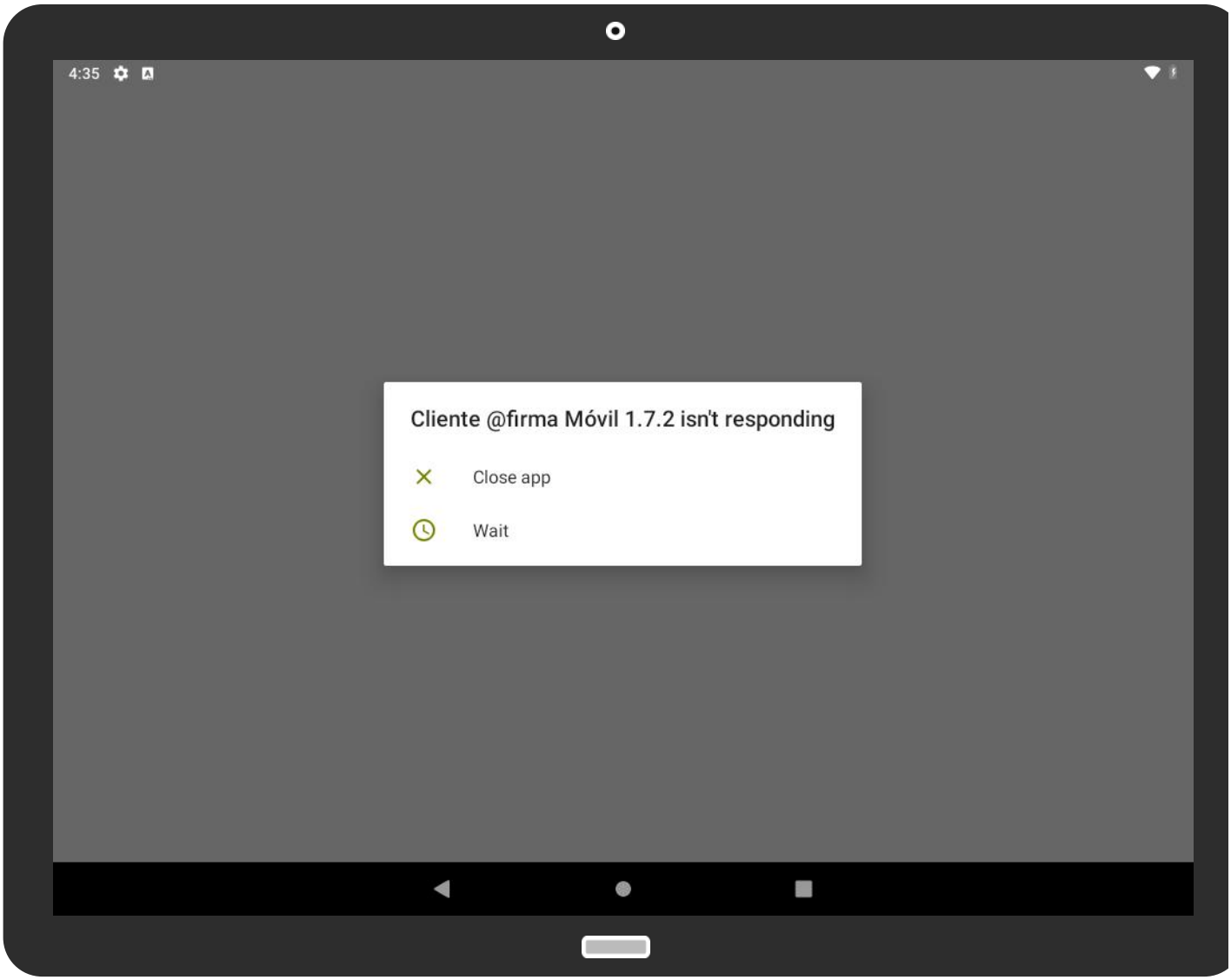
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	OS Credential Dumping	1 System Network Connections Discovery	Remote Services	1 Network Information Discovery	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Cliente m#U00f3vil @firma 1.7.2 1.7.2.apk	0%	ReversingLabs		
Cliente m#U00f3vil @firma 1.7.2 1.7.2.apk	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://ocsp.accv.es0	0%	URL Reputation	safe	
http://ocsp.accv.es0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.acabogacia.org0	0%	URL Reputation	safe	
http://www.color.org	0%	URL Reputation	safe	
http://www.accv.es00	0%	URL Reputation	safe	
http://www.xfa.org/schema/xfa-data/1.0/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.acabogacia.org/crl/aca_arl.crl0	X9.crt	false		unknown
http://crl2.logalty.es/logaltyCARoot03.crl0	aU.cer	false		high
http://ocsp.firmaprofesional.com0	zH.cer, Bp.cer	false		unknown
http://crl.logalty.es/logaltyCARoot.crl0	83.cer	false		high
https://www.logalty.es/PKI/documentacion/0m	aU.cer	false		high
http://crl.firmaprofesional.com/fproot.crl0	zH.cer, Bp.cer	false		high
http://www.acabogacia.org/doc0	X9.crt, lx.crt	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.accv.es/legislacion_c.htm0U	Jb.crt, GM.crt, Yo.crt	false		high
http://www.aiim.org/pdfa/ns/id/	classes.dex, android	false		high
http://ocspfnmtssr.cert.fnmt.es/ocspssr/OcspResponder0E	qf.cer	false		high
https://administracion.gob.es/pag_Home/politicaDePrivacidad.html	resources.arsc, android	false		unknown
http://ocsp.accv.es0	Jb.crt, GM.crt, Yo.crt	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.dnie.es/dpc0	ACRAIZ-SHA2.crt	false	• URL Reputation: safe	unknown
http://www.acabogacia.org0	lx.crt	false	• URL Reputation: safe	unknown
http://www.firmaprofesional.com/cps0	3S.cer, U9.crt	false		high
http://www.color.org	classes.dex, android	false	• URL Reputation: safe	unknown
http://crl1.logalty.es/logaltyCARoot03.crl00	aU.cer	false		high
http://ocsp.redabogacia.org0?	X9.crt	false		unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.firmaprofesional.com/cps0/	zH.cer, Bp.cer	false		high
http://crt.logalty.es/certificateauthority/Logalty CAROOT03.cacert.crt0#	aU.cer	false		high
http://www.cert.fnmt.es/certs/ACRAIZFNMTRCM.crt0	ZT.cer	false		high
http://www.cert.fnmt.es/certs/ACRAIZSERV IDORESSEGUROS.crt0F	qf.cer	false		high
http://www.firmaprofesional.com/cps0;	zH.cer, Bp.cer	false		high
http://schemas.android.com/apk/res/android	qy1.xml, AndroidManifest.xml, android	false		high
http://ocsp1.logalty.es0J	aU.cer	false		unknown
http://www.accv.es/fileadmin/Archivos/certificados /raizaccv1.crt0	Jb.crt	false		high
http://www.accv.es/fileadmin/Archivos/certificados /raizaccv1_der.crl0	Jb.crt, GM.crt, Yo.crt	false		high
http://crl.firmaprofesional.com/caroot.crt0	zH.cer, Bp.cer	false		high
http://www.cert.fnmt.es/crls/ARLFNMTRCM.crl0	ZT.cer	false		high
http://www.bouncycastle.org)	classes.dex, android	false		low
http://www.accv.es00	Jb.crt, GM.crt, Yo.crt	false	• URL Reputation: safe	unknown
http://www.acabogacia.org/crl/aca_arl.crl	X9.crt	false		unknown
http://ocspfnmtrcmca.cert.fnmt.es/ocspfnmtrcmca/OcspResponder0;	ZT.cer	false		high
http://www.cert.fnmt.es/dpcs/0	h3.cer, ZT.cer	false		high
https://sede.administracion.gob.es/politica_de_firma_anexo_1.pdf	policy.properties	false		unknown
https://sede.administracion.gob.es/PAG_Sede/dam/jcr:b0de3f91-5171-48e2-81f3-5c2407d9c091/politica_fi	policy.properties	false		unknown
http://www.cert.fnmt.es/crls/ARLSERVIDOR ESSEGUROS.crl0	qf.cer	false		high
http://www.acabogacia.org/certificados/aca_root.crt0	X9.crt	false		unknown
http://www.xfa.org/schema/xfa-data/1.0/	classes.dex, android	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	764028
Start date and time:	2022-12-09 10:30:52 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Cliente m#U00f3vil @firma 1.7.2 1.7.2.apk
Cookbook file name:	defaultandroidfilecookbook.jbs
Analysis system description:	Android 9 (Pie)
Analysis Mode:	default
APK Instrumentation enabled:	true
Detection:	CLEAN
Classification:	clean8.andAPK@0/251@0/0

Warnings

- Not all executed log events are in report (maximum 10 identical API calls)
- Not all non-executed APIs are in report
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size exceeded maximum capacity and may have missing dynamic data code.

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	Zip archive data, at least v0.0 to extract, compression method=store
Entropy (8bit):	7.982483443094679
TrID:	• Android Package (27504/1) 56.11% • Java Archive (13504/1) 27.55% • ZIP compressed archive (8000/1) 16.32% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	Cliente m#U00f3vil @firma 1.7.2 1.7.2.apk
File size:	6484324
MD5:	5a9163b46f5c743ed3a84224c195defb
SHA1:	595d00ab197ef314f5872fd5c251727825836238
SHA256:	2b4f1d122c8171dccd799e0356b52dcafefba647c72e5652835e2317425f6094
SHA512:	878128b7c15dc2238e4a704f40f4db756b14b23fb45e14447961e215f03e3e73a162c3cbb6fc98bfce77157773c47b016898f92c2f40402974f5baddfd4be229
SSDEEP:	196608:xlTYfWsmqi1cBmPbyljlDU4bnOcrxcvkxR:xVWvgImP+vU4icmvkxR
TLSH:	74663373F335861ECD7A9171491A11AB2A519CC140AAD305B4CEB37C7BFB69C8F812DA
File Content Preview:	PK.....!.!.....f.....PK.....!.!.f...3...7...9...META-INF/com/android/build/gradle/app-metadata.propertiesK,(.M-ILI,I.K-*....5.3.J.K)..Lq/JL.I

File Icon

Static APK Info

General

Label:	Cliente @firma Mvil 1.7.2
Minimum SDK required:	19

Target SDK required:	30
Version Code:	22
Version Name:	22
Package Name:	es.gob.afirma
Is Activity:	true
Is Receiver:	false
Is Service:	false
Requests System Level Permissions:	false
Play Store Compatible:	true

Activities

Name	Is Entrypoint
es.gob.afirmaes.gob.afirma.android.MainActivity	true
es.gob.afirmaes.gob.afirma.android.NFCDetectorActivity	
es.gob.afirmaes.gob.afirma.android.FileChooserActivity	
es.gob.afirmaes.gob.afirma.android.LocalSignResultActivity	
es.gob.afirmaes.gob.afirma.android.WebSignActivity	
es.gob.afirmaes.gob.afirma.android.WebSelectCertificateActivity	
es.gob.afirmaes.gob.afirma.android.WebSaveDataActivity	
es.gob.afirmaes.gob.afirma.android.SaveDataActivity	

Receivers

Permission Requested

- android.permission.ACCESS_NETWORK_STATE
- android.permission.INTERNET
- android.permission.NFC
- android.permission.USE_CREDENTIALS
- android.permission.WRITE_EXTERNAL_STORAGE
- org.simalliance.openmobileapiAET.SMARTCARD

Certificate

Name:	classes.dex
Issuer:	CN=Cliente @firma,OU=Unknown,O=Gobierno de Espaa,L=Unknown,ST=Unknown,C=ES
Subject:	CN=Cliente @firma,OU=Unknown,O=Gobierno de Espaa,L=Unknown,ST=Unknown,C=ES

Resources

Name	Type	Size
ky.xml	Android binary XML	1204
G1.png	PNG image data, 216 x 216, 8-bit/color RGBA, non-interlaced	6449
uimessages.properties	ASCII text, with CRLF line terminators	686
6z.xml	Android binary XML	548
zH.cer	Certificate, Version=3	1796
kY.gif	GIF image data, version 89a, 1081 x 1930	1119965
Te.cer	PEM certificate	2564
androidx.core_core.version	ASCII text	6
androidx.lifecycle_lifecycle-livedata.version	ASCII text	6
keystoremessages_gl_ES.properties	ASCII text, with CRLF line terminators	2632
-r.png	PNG image data, 81 x 81, 8-bit colormap, non-interlaced	1940
9K.xml	Android binary XML	1728
Ox.png	PNG image data, 72 x 72, 8-bit/color RGBA, non-interlaced	4968
protocolomessages.properties	ASCII text, with CRLF line terminators	47
xs.xml	Android binary XML	1128
Helvetica-Bold.afm	ASCII font metrics	72096
yT.png	PNG image data, 108 x 108, 8-bit colormap, non-interlaced	2181
G9.cer	PEM certificate	2119

Name	Type	Size
7B.xml	Android binary XML	392
cH.cer	PEM certificate	3514
GF.png	PNG image data, 72 x 72, 8-bit/color RGBA, non-interlaced	4761
androidx.annotation_annotation-experimental.version	ASCII text	6
eK.9.png	PNG image data, 8 x 8, 8-bit/color RGB, non-interlaced	223
dnie.png	PNG image data, 400 x 300, 8-bit/color RGBA, non-interlaced	40930
ee.png	PNG image data, 512 x 141, 8-bit/color RGBA, non-interlaced	11972
androidx.versionedparcelable_versionedparcelable.version	ASCII text	6
cardmessages.properties	CSV text	300
X2.png	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced	2365
keystoremessages.properties	ASCII text, with CRLF line terminators	3418
fM.png	PNG image data, 108 x 108, 8-bit colormap, non-interlaced	119
magic_1_0.dtd	ASCII text, with CRLF line terminators	548
Ar.png	PNG image data, 800 x 460, 8-bit colormap, non-interlaced	3431
Qv.png	PNG image data, 15 x 15, 8-bit/color RGB, non-interlaced	98
_C.png	PNG image data, 324 x 324, 8-bit/color RGBA, non-interlaced	10401
Courier-Bold.afm	ASCII font metrics	15675
Vw.png	PNG image data, 432 x 432, 8-bit colormap, non-interlaced	288
AR.png	PNG image data, 144 x 144, 8-bit colormap, non-interlaced	4566
fT.png	PNG image data, 72 x 72, 8-bit/color RGBA, non-interlaced	4968
can_example.png	PNG image data, 798 x 530, 8-bit/color RGBA, non-interlaced	754362
Helvetica-Oblique.afm	ASCII font metrics	77443
Times-BoldItalic.afm	ASCII font metrics	62026
policy.properties	ASCII text, with CRLF line terminators	1661
iL.xml	Targa image data - RLE 196 x 65536 x 8 +1 +28 ""	440
classes.dex	Dalvik dex file version 035	7162320
FZ.xml	Android binary XML	532
Ot.png	PNG image data, 30 x 30, 8-bit/color RGB, non-interlaced	138
enhancer.properties	ASCII text, with CRLF line terminators	239
cq.xml	Android binary XML	2732
rF.xml	Targa image data - RLE 176 x 65536 x 8 +1 +28 ""	456
66.png	PNG image data, 72 x 72, 8-bit/color RGBA, non-interlaced	4761
gj.png	PNG image data, 72 x 72, 8-bit/color RGB, non-interlaced	4058
app-metadata.properties	ASCII text	55
dnie_logo.png	PNG image data, 64 x 42, 8-bit colormap, non-interlaced	2227
aA.xml	Android binary XML	612
Courier.afm	ASCII font metrics	15677
WF.png	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced	1969
fi.xml	Android binary XML	552
hj.9.png	PNG image data, 8 x 8, 8-bit grayscale, non-interlaced	215
Jb.crt	Certificate, Version=3	2007
logo.gif	GIF image data, version 89a, 38 x 26	964
Helvetica-BoldOblique.afm	ASCII font metrics	72192
qf.cer	Certificate, Version=3	905
jb.png	PNG image data, 81 x 81, 8-bit colormap, non-interlaced	1773
gD.cer	PEM certificate	2136
aH.png	PNG image data, 324 x 324, 8-bit/color RGBA, non-interlaced	12523
zf.png	PNG image data, 120 x 120, 8-bit/color RGBA, non-interlaced	18754
glyphlist.txt	ASCII text, with CRLF line terminators	101224
Cv1.xml	Android binary XML	2652
CERT.RSA	data	1413
jB.xml	Targa image data - RLE 144 x 65536 x 8 +1 +28 ""	420
Bp.cer	Certificate, Version=3	1661
Symbol.afm	ASCII font metrics	9953
Xs.9.png	PNG image data, 12 x 12, 8-bit/color RGB, non-interlaced	225
C7.xml	Android binary XML	2456
jp.xml	Android binary XML	2784
h3.cer	Certificate, Version=3	1415

Name	Type	Size
Vz.xml	Android binary XML	2764
LICENSE-junit.txt	ASCII text	11376
dn.png	PNG image data, 162 x 162, 8-bit colormap, non-interlaced	3059
8V.9.png	PNG image data, 16 x 16, 8-bit grayscale, non-interlaced	221
resources.arsc	data	91376
magic.xml	XML 1.0 document, ASCII text, with very long lines (65413), with CRLF line terminators	95554
CERT.SF	ASCII text, with CRLF line terminators	20627
5Q.png	PNG image data, 144 x 144, 8-bit/color RGBA, non-interlaced	12256
u3.png	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced	2210
ACRAIZ-SHA2-2.crt	PEM certificate	2124
93.9.png	PNG image data, 16 x 16, 8-bit/color RGB, non-interlaced	247
ZapfDingbats.afm	ASCII font metrics	9752
p9.png	PNG image data, 162 x 162, 8-bit/color RGBA, non-interlaced	5210
WB.png	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced	1431
4w.xml	Targa image data - RLE 60 x 65536 x 1 +1 +28 ""	136
5X.png	PNG image data, 96 x 96, 8-bit/color RGBA, non-interlaced	4006
ZT.cer	Certificate, Version=3	1754
androidx.customview_customview.version	ASCII text	6
GM.crt	Certificate, Version=3	1917
4W.xml	Android binary XML	1228
Ke.png	PNG image data, 216 x 216, 8-bit/color RGBA, non-interlaced	7613
rP.png	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced	2599
Cz.xml	Android binary XML	1040
androidx.arch.core_core-runtime.version	ASCII text	6
LM.png	PNG image data, 192 x 192, 8-bit colormap, non-interlaced	6017
X9.crt	Certificate, Version=3	1833
PF.xml	Android binary XML	1128
vP.xml	Android binary XML	1144
smalllogo.gif	GIF image data, version 89a, 22 x 17	883
dj.png	PNG image data, 460 x 800, 8-bit colormap, non-interlaced	5979
5m.png	PNG image data, 108 x 108, 8-bit/color RGBA, non-interlaced	3264
jL.xml	Android binary XML	548
Yo.crt	Certificate, Version=3	1942
androidx.lifecycle_lifecycle-viewmodel-savedstate.version	ASCII text	6
Tm.xml	Android binary XML	2556
Helvetica.afm	ASCII font metrics	77343
q6.xml	Android binary XML	1180
jmulticardmessages_gl_ES.properties	ASCII text, with CRLF line terminators	865
CertPathReviewerMessages.properties	ASCII text, with very long lines (533)	42868
EQ.xml	Android binary XML	572
SI.png	PNG image data, 48 x 48, 8-bit/color RGB, non-interlaced	2630
u6.xml	Android binary XML	392
NR.xml	Android binary XML	372
androidx.viewpager_viewpager.version	ASCII text	6
Bn.xml	Targa image data - RLE 328 x 65536 x 15 +1 +28 ""	1028
Cv.xml	Android binary XML	304
09.9.png	PNG image data, 12 x 12, 8-bit grayscale, non-interlaced	212
SS.xml	Android binary XML	988
Go.png	PNG image data, 72 x 72, 8-bit/color RGBA, non-interlaced	3014
qK.xml	Android binary XML	364
ze.png	PNG image data, 120 x 120, 8-bit/color RGBA, non-interlaced	17645
T2.9.png	PNG image data, 12 x 12, 8-bit/color RGB, non-interlaced	225
Am.png	PNG image data, 80 x 80, 8-bit/color RGBA, non-interlaced	9463
Pi.xml	Targa image data - RLE 44 x 65536 x 1 +1 +28 ""	120
qy.xml	Android binary XML	616

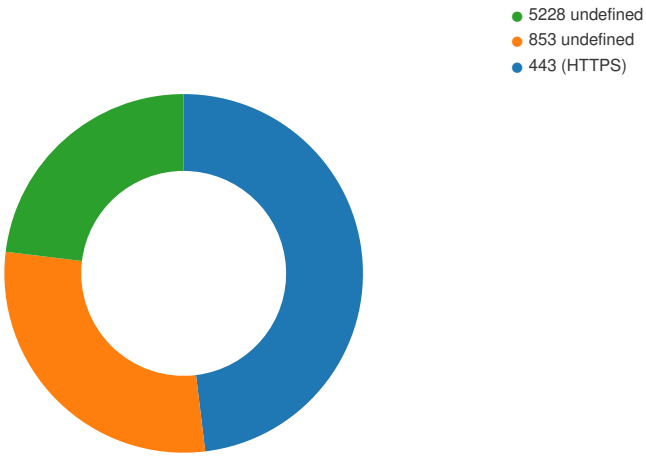
Name	Type	Size
fv.png	PNG image data, 959 x 75, 8-bit colormap, non-interlaced	164
7y.png	PNG image data, 96 x 96, 8-bit/color RGB, non-interlaced	5585
3S.cer	Certificate, Version=3	1560
CertPathReviewerMessages_de.properties	ISO-8859 text, with very long lines (376)	49608
Ze.cer	PEM certificate	2586
fp.cer	PEM certificate	2647
nh.png	PNG image data, 32 x 32, 8-bit gray+alpha, non-interlaced	374
commonpdfmessages_gl_ES.properties	ASCII text, with CRLF line terminators	349
Times-Italic.afm	ASCII font metrics	68995
tJ.xml	Android binary XML	604
androidx.lifecycle_lifecycle-viewmodel.version	ASCII text	6
jK.9.png	PNG image data, 12 x 12, 8-bit grayscale, non-interlaced	212
_F.cer	PEM certificate	2108
Times-Roman.afm	ASCII font metrics	62879
SH.xml	Targa image data - RLE 196 x 65536 x 8 +1 +28 ""	440
JU.png	PNG image data, 81 x 81, 8-bit gray+alpha, non-interlaced	93
YQ.xml	Android binary XML	452
U9.crt	Certificate, Version=3	1560
TJ.cer	PEM certificate	1942
androidx.lifecycle_lifecycle-livedata-core.version	ASCII text	6
DS.xml	Android binary XML	1052
androidx.loader_loader.version	ASCII text	6
template.xml	XML 1.0 document, ASCII text, with very long lines (633), with CRLF line terminators	756
androidx.lifecycle_lifecycle-runtime.version	ASCII text	6
qG.xml	Android binary XML	2684
tr.9.png	PNG image data, 16 x 16, 8-bit/color RGB, non-interlaced	252
Ru.xml	Targa image data - RLE 328 x 65536 x 15 +1 +28 ""	1028
GK.xml	Android binary XML	3256
MANIFEST.MF	ASCII text, with CRLF line terminators	20553
chipcard.png	PNG image data, 200 x 170, 8-bit/color RGBA, non-interlaced	141689
h4.png	PNG image data, 64 x 64, 8-bit gray+alpha, non-interlaced	681
Ap.png	PNG image data, 80 x 80, 8-bit/color RGBA, non-interlaced	9883
tf.png	PNG image data, 72 x 72, 8-bit/color RGBA, non-interlaced	5408
jmulticardmessages.properties	ASCII text, with CRLF line terminators	864
b2.png	PNG image data, 432 x 432, 8-bit/color RGBA, non-interlaced	17689
ACRAIZ-SHA2.crt	Certificate, Version=3	1475
fR.png	PNG image data, 324 x 324, 8-bit colormap, non-interlaced	210
C9.png	PNG image data, 192 x 192, 8-bit/color RGBA, non-interlaced	17728
R5.xml	Android binary XML	2616
uu.xml	Android binary XML	1844
androidsupportmultidexversion.txt	ASCII text	53
dp.xml	Android binary XML	1128
1S.png	PNG image data, 96 x 96, 8-bit/color RGBA, non-interlaced	7711
restore.png	PNG image data, 300 x 300, 8-bit colormap, non-interlaced	3524
jy.png	PNG image data, 96 x 96, 8-bit/color RGBA, non-interlaced	4510
UT.xml	Android binary XML	3208
SD.png	PNG image data, 72 x 72, 8-bit/color RGBA, non-interlaced	3307
cmap_info.txt	ASCII text, with CRLF line terminators	5303
Times-Bold.afm	ASCII font metrics	66839
VV.cer	PEM certificate	3996
5z.png	PNG image data, 48 x 48, 8-bit gray+alpha, non-interlaced	535
Dv.xml	Targa image data - RLE 216 x 65536 x 8 +1 +28 ""	664
CG.png	PNG image data, 192 x 192, 8-bit/color RGBA, non-interlaced	10031
7c.png	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced	3317
jS.cer	PEM certificate	2156
mrzcountrycodes.properties	ASCII text, with CRLF line terminators	4193

Name	Type	Size
androidx.tracing_tracing.version	ASCII text	6
8r.xml	Android binary XML	1156
jmulticardprovidermessages.properties	ASCII text, with CRLF line terminators	136
lx.crt	Certificate, Version=3	1216
tb.xml	Android binary XML	452
WR.png	PNG image data, 216 x 216, 8-bit colormap, non-interlaced	153
fu.xml	Android binary XML	1564
PH.xml	Android binary XML	548
BT.png	PNG image data, 256 x 71, 8-bit/color RGBA, non-interlaced	5708
dH.9.png	PNG image data, 16 x 16, 8-bit grayscale, non-interlaced	221
RX.png	PNG image data, 162 x 162, 8-bit colormap, non-interlaced	133
androidx.fragment_fragment.version	ASCII text	6
dE.png	PNG image data, 72 x 72, 8-bit/color RGBA, non-interlaced	3014
Pq.9.png	PNG image data, 8 x 8, 8-bit grayscale, non-interlaced	215
83.cer	Certificate, Version=3	1729
oO.png	PNG image data, 72 x 72, 8-bit/color RGBA, non-interlaced	3014
androidx.savedstate_savedstate.version	ASCII text	6
mimetypes_oids.properties	ASCII text, with CRLF line terminators	607
NF.png	PNG image data, 432 x 432, 8-bit/color RGBA, non-interlaced	14602
aU.cer	Certificate, Version=3	1983
uimessages_gl_ES.properties	ASCII text, with CRLF line terminators	658
Tv.xml	Android binary XML	2660
nu.xml	Targa image data - RLE 616 x 65536 x 32 +1 +28 ""	2812
4N.xml	Targa image data - RLE 304 x 65536 x 16 +1 +28 ""	908
3m.xml	Android binary XML	532
BB.xml	Android binary XML	1332
4u.xml	Android binary XML	2508
bJ.xml	Targa image data - RLE 328 x 65536 x 15 +1 +28 ""	1028
kd.png	PNG image data, 36 x 36, 8-bit/color RGBA, non-interlaced	1504
qm.xml	Android binary XML	2652
LD.png	PNG image data, 14 x 14, 8-bit/color RGB, non-interlaced	107
Courier-BoldOblique.afm	ASCII font metrics	15741
O3.9.png	PNG image data, 8 x 8, 8-bit/color RGB, non-interlaced	223
mG.cer	Certificate, Version=3	626
D2.png	PNG image data, 144 x 144, 8-bit/color RGBA, non-interlaced	7069
maximize.png	PNG image data, 300 x 300, 8-bit colormap, non-interlaced	2434
s6.xml	Android binary XML	1128
5d.xml	Android binary XML	1232
commonpdfmessages.properties	HTML document, ASCII text, with CRLF line terminators	387
N4.png	PNG image data, 798 x 530, 8-bit/color RGB, non-interlaced	670709
Courier-Oblique.afm	ASCII font metrics	15783
qy1.xml	Android binary XML	580
androidx.activity_activity.version	ASCII text	6
AndroidManifest.xml	Android binary XML	8764

Network Behavior

Network Port Distribution

Total Packets: 52



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:31:10.426767111 CET	50458	443	192.168.2.30	216.58.212.170
Dec 9, 2022 10:31:10.554752111 CET	39602	443	192.168.2.30	142.250.186.163
Dec 9, 2022 10:31:14.330909014 CET	50458	443	192.168.2.30	216.58.212.170
Dec 9, 2022 10:31:14.587163925 CET	39602	443	192.168.2.30	142.250.186.163
Dec 9, 2022 10:31:22.459791899 CET	50458	443	192.168.2.30	216.58.212.170
Dec 9, 2022 10:31:22.971832991 CET	39602	443	192.168.2.30	142.250.186.163
Dec 9, 2022 10:31:38.333992958 CET	50458	443	192.168.2.30	216.58.212.170
Dec 9, 2022 10:31:39.357079983 CET	39602	443	192.168.2.30	142.250.186.163
Dec 9, 2022 10:32:05.832348108 CET	50870	443	192.168.2.30	142.250.186.42
Dec 9, 2022 10:32:08.110531092 CET	56068	853	192.168.2.30	8.8.4.4
Dec 9, 2022 10:32:08.129204035 CET	853	56068	8.8.4.4	192.168.2.30
Dec 9, 2022 10:32:08.129426956 CET	56068	853	192.168.2.30	8.8.4.4
Dec 9, 2022 10:32:08.132561922 CET	56068	853	192.168.2.30	8.8.4.4
Dec 9, 2022 10:32:08.149559021 CET	853	56068	8.8.4.4	192.168.2.30
Dec 9, 2022 10:32:08.157289028 CET	853	56068	8.8.4.4	192.168.2.30
Dec 9, 2022 10:32:08.157330990 CET	853	56068	8.8.4.4	192.168.2.30
Dec 9, 2022 10:32:08.157356977 CET	853	56068	8.8.4.4	192.168.2.30
Dec 9, 2022 10:32:08.157409906 CET	853	56068	8.8.4.4	192.168.2.30
Dec 9, 2022 10:32:08.157533884 CET	56068	853	192.168.2.30	8.8.4.4
Dec 9, 2022 10:32:08.157533884 CET	56068	853	192.168.2.30	8.8.4.4
Dec 9, 2022 10:32:08.161545038 CET	56068	853	192.168.2.30	8.8.4.4
Dec 9, 2022 10:32:08.175004005 CET	56068	853	192.168.2.30	8.8.4.4
Dec 9, 2022 10:32:08.192570925 CET	853	56068	8.8.4.4	192.168.2.30
Dec 9, 2022 10:32:08.192851067 CET	56068	853	192.168.2.30	8.8.4.4
Dec 9, 2022 10:32:08.215261936 CET	853	56068	8.8.4.4	192.168.2.30
Dec 9, 2022 10:32:08.219089985 CET	853	56068	8.8.4.4	192.168.2.30
Dec 9, 2022 10:32:08.220659018 CET	39732	5228	192.168.2.30	108.177.126.188
Dec 9, 2022 10:32:08.247416019 CET	5228	39732	108.177.126.188	192.168.2.30
Dec 9, 2022 10:32:08.247662067 CET	39732	5228	192.168.2.30	108.177.126.188
Dec 9, 2022 10:32:08.249839067 CET	39732	5228	192.168.2.30	108.177.126.188
Dec 9, 2022 10:32:08.259594917 CET	56068	853	192.168.2.30	8.8.4.4
Dec 9, 2022 10:32:08.276700974 CET	5228	39732	108.177.126.188	192.168.2.30
Dec 9, 2022 10:32:08.276781082 CET	5228	39732	108.177.126.188	192.168.2.30
Dec 9, 2022 10:32:08.276868105 CET	5228	39732	108.177.126.188	192.168.2.30
Dec 9, 2022 10:32:08.276911020 CET	5228	39732	108.177.126.188	192.168.2.30
Dec 9, 2022 10:32:08.276956081 CET	5228	39732	108.177.126.188	192.168.2.30
Dec 9, 2022 10:32:08.277000904 CET	5228	39732	108.177.126.188	192.168.2.30
Dec 9, 2022 10:32:08.277040005 CET	5228	39732	108.177.126.188	192.168.2.30
Dec 9, 2022 10:32:08.277045012 CET	39732	5228	192.168.2.30	108.177.126.188
Dec 9, 2022 10:32:08.277045965 CET	39732	5228	192.168.2.30	108.177.126.188
Dec 9, 2022 10:32:08.277045965 CET	39732	5228	192.168.2.30	108.177.126.188

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:32:08.277045965 CET	39732	5228	192.168.2.30	108.177.126.188
Dec 9, 2022 10:32:08.277153015 CET	39732	5228	192.168.2.30	108.177.126.188
Dec 9, 2022 10:32:08.277153015 CET	39732	5228	192.168.2.30	108.177.126.188
Dec 9, 2022 10:32:08.289705992 CET	39732	5228	192.168.2.30	108.177.126.188
Dec 9, 2022 10:32:08.321763992 CET	5228	39732	108.177.126.188	192.168.2.30
Dec 9, 2022 10:32:08.322020054 CET	39732	5228	192.168.2.30	108.177.126.188
Dec 9, 2022 10:32:08.348983049 CET	5228	39732	108.177.126.188	192.168.2.30
Dec 9, 2022 10:32:08.349077940 CET	5228	39732	108.177.126.188	192.168.2.30
Dec 9, 2022 10:32:08.359246969 CET	5228	39732	108.177.126.188	192.168.2.30
Dec 9, 2022 10:32:08.359338045 CET	5228	39732	108.177.126.188	192.168.2.30
Dec 9, 2022 10:32:08.388082981 CET	39732	5228	192.168.2.30	108.177.126.188
Dec 9, 2022 10:32:08.429229975 CET	56068	853	192.168.2.30	8.8.4.4
Dec 9, 2022 10:32:08.451250076 CET	853	56068	8.8.4.4	192.168.2.30
Dec 9, 2022 10:32:08.455914974 CET	853	56068	8.8.4.4	192.168.2.30
Dec 9, 2022 10:32:08.456186056 CET	56068	853	192.168.2.30	8.8.4.4
Dec 9, 2022 10:32:08.471323013 CET	47664	443	192.168.2.30	142.251.209.46
Dec 9, 2022 10:32:08.471381903 CET	443	47664	142.251.209.46	192.168.2.30
Dec 9, 2022 10:32:08.471549988 CET	47664	443	192.168.2.30	142.251.209.46
Dec 9, 2022 10:32:08.473769903 CET	47664	443	192.168.2.30	142.251.209.46
Dec 9, 2022 10:32:08.473820925 CET	443	47664	142.251.209.46	192.168.2.30
Dec 9, 2022 10:32:08.555948973 CET	443	47664	142.251.209.46	192.168.2.30
Dec 9, 2022 10:32:08.556132078 CET	47664	443	192.168.2.30	142.251.209.46
Dec 9, 2022 10:32:08.556559086 CET	47664	443	192.168.2.30	142.251.209.46
Dec 9, 2022 10:32:08.556583881 CET	443	47664	142.251.209.46	192.168.2.30
Dec 9, 2022 10:32:08.557190895 CET	443	47664	142.251.209.46	192.168.2.30
Dec 9, 2022 10:32:08.558491945 CET	443	47664	142.251.209.46	192.168.2.30
Dec 9, 2022 10:32:08.561254978 CET	47664	443	192.168.2.30	142.251.209.46
Dec 9, 2022 10:32:08.561284065 CET	443	47664	142.251.209.46	192.168.2.30
Dec 9, 2022 10:32:08.601588964 CET	47664	443	192.168.2.30	142.251.209.46
Dec 9, 2022 10:32:08.622368097 CET	47664	443	192.168.2.30	142.251.209.46
Dec 9, 2022 10:32:08.622412920 CET	443	47664	142.251.209.46	192.168.2.30
Dec 9, 2022 10:32:08.622952938 CET	443	47664	142.251.209.46	192.168.2.30
Dec 9, 2022 10:32:08.623064041 CET	47664	443	192.168.2.30	142.251.209.46
Dec 9, 2022 10:32:08.623084068 CET	443	47664	142.251.209.46	192.168.2.30
Dec 9, 2022 10:32:08.623157024 CET	47664	443	192.168.2.30	142.251.209.46
Dec 9, 2022 10:32:08.625674963 CET	47664	443	192.168.2.30	142.251.209.46
Dec 9, 2022 10:32:08.625691891 CET	443	47664	142.251.209.46	192.168.2.30
Dec 9, 2022 10:32:08.734683037 CET	443	47664	142.251.209.46	192.168.2.30
Dec 9, 2022 10:32:08.735034943 CET	443	47664	142.251.209.46	192.168.2.30
Dec 9, 2022 10:32:08.736017942 CET	47664	443	192.168.2.30	142.251.209.46
Dec 9, 2022 10:32:08.736074924 CET	443	47664	142.251.209.46	192.168.2.30
Dec 9, 2022 10:32:08.736124992 CET	47664	443	192.168.2.30	142.251.209.46
Dec 9, 2022 10:32:09.567706108 CET	50458	443	192.168.2.30	216.58.212.170
Dec 9, 2022 10:32:11.615842104 CET	39602	443	192.168.2.30	142.250.186.163
Dec 9, 2022 10:32:23.464822054 CET	56068	853	192.168.2.30	8.8.4.4
Dec 9, 2022 10:32:23.481292963 CET	853	56068	8.8.4.4	192.168.2.30
Dec 9, 2022 10:32:28.478101969 CET	56068	853	192.168.2.30	8.8.4.4
Dec 9, 2022 10:32:28.478218079 CET	56068	853	192.168.2.30	8.8.4.4
Dec 9, 2022 10:32:28.495172977 CET	853	56068	8.8.4.4	192.168.2.30
Dec 9, 2022 10:32:28.495780945 CET	56068	853	192.168.2.30	8.8.4.4
Dec 9, 2022 10:35:19.882215023 CET	54604	443	192.168.2.30	142.250.186.138
Dec 9, 2022 10:35:19.882256985 CET	443	54604	142.250.186.138	192.168.2.30

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 9, 2022 10:33:52.617851973 CET	68	67	192.168.2.30	192.168.2.1
Dec 9, 2022 10:33:52.618223906 CET	67	68	192.168.2.1	192.168.2.30

HTTP Request Dependency Graph

- android.clients.google.com

APK Behavior

Miscellaneous

Simulated Events

Type	Data
boot completed	-
time tick	-
incoming sms	0123456789 this is a text message
outgoing sms	9876543210 thank you
location change	54.13 12.14
motion simulation	-
incoming call	0123456789
outgoing call	9876543210
time tick	-

Interacted Views

View Data

- Object: android.widget.Button{919b18a VFED..C.. .F..... 352,0-484,48 #7f07002a app:id/buttonSign}
- X: 418
- Y: 629
- Label: Sign local file

Disassembly

0 Executed Methods

0 Non-Executed Methods