Device name: android-53144dd969f50300
Device MAC address: bc:bd:9e:2c:2c:f6
Report generated on 04/04/2021 - 20:47:09
Capture duration: 361.494415298 seconds
Number of packets: 19999
Capture SHA1: 33dda0c69886b666b84af0e8a01f8c6c4368443b

TinyCheck

You have one moderate alert(s), your device might be compromised. Please look at them carefully.

MODERATE SSL-02

An SSL connection to ds.shalltry.com is using a free certificate.

Free certificates — such as Let's Encrypt — are wildly used by command and control servers associated to malicious implants or phishing web pages. We recommend to check the host associated to this certificate, by looking at the domain name, its creation date, or by checking its reputation on the internet.

Suspect communications

Protocol	Domain	Dst IP address	Dst port number
TCP	ds.shalltry.com	34.250.49.239	443

Whitelisted communications

Protocol	Domain	Dst IP address	Dst port number
UDP	--	192.168.100.1	53
UDP	--	192.168.100.1	67
UDP	2.android.pool.ntp.org	80.249.145.122	123
UDP	2.android.pool.ntp.org	84.16.73.33	123
UDP	2.android.pool.ntp.org	116.66.161.5	123
UDP	2.android.pool.ntp.org	195.24.196.113	123
UDP	2.android.pool.ntp.org	188.125.64.7	123
UDP	--	224.0.0.251	5353
UDP	--	255.255.255.255	67
UDP	android.clients.google.com	172.217.18.206	443

Protocol	Domain	Dst IP address	Dst port number
UDP	android.clients.google.com	216.58.204.142	443
UDP	android.clients.google.com	216.58.214.78	443
TCP	android.clients.google.com	216.58.204.142	443
TCP	android.clients.google.com	172.217.18.206	443
TCP	android.clients.google.com	142.250.74.238	443
UDP	android.clients.google.com	142.250.74.238	443
TCP	android.googleapis.com	216.58.204.138	443
UDP	android.googleapis.com	216.58.204.138	443
UDP	app-measurement.com	172.217.22.142	443
TCP	app-measurement.com	172.217.22.142	443
TCP	beacons.gcp.gvt2.com	216.58.213.163	443
UDP	beacons.gcp.gvt2.com	216.58.213.163	443
TCP	beacons.gvt2.com	172.217.18.195	443
UDP	beacons.gvt2.com	172.217.18.195	443
TCP	connectivitycheck.gstatic.com	216.58.213.131	80
TCP	connectivitycheck.gstatic.com	216.58.213.131	443
UDP	--	ff02::fb	5353
TCP	firebaseinstallations.googleapis.com	216.58.206.234	443
TCP	firebaseinstallations.googleapis.com	216.58.206.234	443
TCP	fonts.gstatic.com	216.58.215.35	443
TCP	footprints-pa.googleapis.com	172.217.22.138	443
TCP	googleads.g.doubleclick.net	216.58.213.66	443
UDP	i.ytimg.com	172.217.19.246	443
TCP	inbox.google.com	142.250.179.101	443
TCP	lh3.googleusercontent.com	216.58.213.161	443
TCP	mail.google.com	216.58.204.133	443
TCP	mtalk.google.com	64.233.166.188	5228
TCP	notifications-pa.googleapis.com	216.58.213.170	443

Protocol	Domain	Dst IP address	Dst port number
UDP	notifications-pa.googleapis.com	216.58.213.170	443
UDP	play-lh.googleusercontent.com	216.58.214.86	443
UDP	play.googleapis.com	216.58.209.234	443
TCP	play.googleapis.com	216.58.209.234	443
UDP	r1---sn-25ge7nsk.gvt1.com	173.194.190.166	443
UDP	r3---sn-25glen7r.gvt1.com	74.125.105.89	443
UDP	r5---sn-25glenes.gvt1.com	173.194.190.74	443
TCP	rcs-acs-mcc624.jibe.google.com	216.239.36.155	443
TCP	searchlite-pa.googleapis.com	142.250.74.234	443
UDP	searchlite-pa.googleapis.com	142.250.74.234	443
TCP	wallet.google.com	74.125.206.92	443
UDP	www.google.com	172.217.22.132	443
TCP	www.google.com	172.217.22.132	443
TCP	www.googleapis.com	216.58.214.74	443
TCP	www.googleapis.com	172.217.19.234	443
TCP	www.googleapis.com	142.250.179.74	443
TCP	www.googleapis.com	142.250.179.106	443
UDP	www.googleapis.com	142.250.179.106	443
UDP	www.googleapis.com	142.250.179.74	443
UDP	www.googleapis.com	216.58.198.202	443
UDP	www.gstatic.com	142.250.179.99	443
TCP	www.gstatic.com	142.250.179.99	443
UDP	youtubei.googleapis.com	216.58.201.234	443
TCP	youtubei.googleapis.com	216.58.201.234	443