Device name: android-53144dd969f50300
Device MAC address: bc:bd:9e:2c:2c:f6
Report generated on 04/04/2021 - 20:47:57
Capture duration: 465.144533476 seconds
Number of packets: 486
Capture SHA1: 54eb12d8107ce9a3eda54d974e97a6bcd90c6eee

Your device seems to be compromised as you have one high alert(s).

HIGH IOC-03

A DNS request have been done to www.cerberusapp.com which is tagged as STALKERWARE.

The domain name www.cerberusapp.com seen in the capture has been explicitly tagged as malicious. This indicates that your device is likely compromised and needs to be investigated deeply.

LOW PROTO-03

HTTP communications have been done to the host www.cerberusapp.com

Your device exchanged with the host www.cerberusapp.com by using HTTP, an unencrypted protocol. Even if this behavior is not malicious by itself, it is unusual to see HTTP communications issued from smartphone applications running in the background. Please check the host reputation by searching it on the internet.

Suspect communications

Protocol	Domain	Dst IP address	Dst port number
TCP	www.cerberusapp.com	66.228.35.203	80
TCP	www.cerberusapp.com	66.228.35.203	443

Whitelisted communications

Protocol	Domain	Dst IP address	Dst port number
UDP	--	192.168.100.1	67
UDP	--	192.168.100.1	53
UDP	--	192.168.100.255	8610
UDP	--	192.168.100.255	8612
UDP	--	224.0.0.251	5353

Protocol	Domain	Dst IP address	Dst port number
UDP	--	255.255.255.255	67
TCP	connectivitycheck.gstatic.com	216.58.215.35	80
TCP	connectivitycheck.gstatic.com	216.58.215.35	80
TCP	connectivitycheck.gstatic.com	216.58.215.35	443
UDP	--	ff02::1	8612
UDP	--	ff02::1	8610
UDP	--	ff02::fb	5353
TCP	inbox.google.com	142.250.74.229	443
TCP	infinitedata-pa.googleapis.com	142.250.74.234	443
TCP	mtalk.google.com	64.233.167.188	5228
TCP	www.google.com	216.58.198.196	443