Emergency VPN Automated Report

This is an automated report of your Emergency VPN session generated with the Civilsphere AI VPN technology (beta). One of our analysts will review your session and send a follow-up report within the next 30 days.

If you are in need of immediate assistance, please contact AccessNow Helpline indicating that you already made the assessment with the Emergency VPN: https://www.accessnow.org/help/.

Capture 20210803140814-talk_warm_192.168.255.222_03258457

Capture Information

```
File name: 20210803140814-talk_warm_192.168.255.222_03258457.pcap
Number of packets: 22140
File size (bytes): 15468140
Start time: 2021-08-03 14:11:16.959136
End time: 2021-08-03 14:32:51.744783
SHA256: a158c202b8b845fd7b58dc385dd0b102ceb77b5c8d182ad8f7db1da1a47ab6c8
```

Top Data Transfers (bytes)

Malicious applications usually steal data (photos, messages, files, voice recordings) from the device. The stolen data is uploaded to malicious servers. Recognizing which services the device is sending data to is important to identify possible malicious activity.

If you do not recognize any of the services listed below and you are a person at risk, we recommend factory resetting the device to remove any suspicious activity. Be advised that a factory reset will not fix a compromised account (email, iCloud, Google, etc.).

These are the top 10 data transfers:

A <->B	ASN	B ->A (bytes)	A ->B (bytes)	Total Transferred (bytes)	Total Duration (seconds)
157.240.30.63 <->192.168.255.222	FACEBOOK, US	229785	5800420	6030205	421.9972
68.232.34.217 <->192.168.255.222	EDGECAST, US	105790	4081307	4187097	767.2869
172.217.23.238 <->192.168.255.222	GOOGLE, US	32370	701423	733793	6.7724
157.240.30.27 <->192.168.255.222	FACEBOOK, US	10360	245793	256153	394.8589
172.217.23.197 <->192.168.255.222	GOOGLE, US	75670	150245	225915	715.6925
93.184.220.70 <->192.168.255.222	EDGECAST, US	10300	127198	137498	32.7003
172.217.23.202 <->192.168.255.222	GOOGLE, US	69947	115220	185167	714.3312
23.47.212.26 <->192.168.255.222	AKAMAI-AS, US	33679	97492	131171	99.1507
192.168.255.222 <->216.58.201.74	Unknown	95408	79649	175057	692.7084
192.168.255.222 <->209.237.200.128	Unknown	134230	74207	208437	705.1233

Top Resolved DNS Requests

DNS is essential to network communications, and malware also relies on DNS to resolve addresses where to connect. DNS could also be used to tunnel data and steal information. Additionally, DNS helps identify the services the device is using. These are the top 30 DNS domains resolved in this session:

- 122 powerful-horse-flps3z71ccv91oiuzvtrhm77[.]herokudns[.]com
- 30 gateway[.]fe[.]apple-dns[.]net
- 18 www[.]googleapis[.]com
- 16 www[.]google[.]com
- 16 oauthaccountmanager[.]googleapis[.]com
- 12 inappcheck[.]itunes[.]apple[.]com
- 12 api-0-4-6[.]twitter[.]com
- 12 connectivitycheck[.]gstatic[.]com
- 12 pbs[.]twimg[.]com
- 12 abs[.]twimg[.]com
- 12 api[.]twitter[.]com
- 12 api-46-0-0[.]twitter[.]com
- 10 inbox[.]google[.]com
- 8 www[.]icloud[.]com
- 8 apple[.]com
- 8 mobilemaps[.]googleapis[.]com
- 8 gateway[.]icloud[.]com
- 8 weather-data[.]apple[.]com
- 8 a2047[.]dscb[.]akamai[.]net
- 8 app-measurement[.]com

- 8 portal[.]iverify[.]io
- 8 video[.]twimg[.]com
- 8 e69896[.]dscapi6[.]akamaiedge[.]net
- 8 mail[.]google[.]com
- 8 mail-attachment[.]googleusercontent[.]com
- 8 api-20-0-0[.]twitter[.]com
- 8 api-34-0-0[.]twitter[.]com
- 8 dc[.]albtls[.]t[.]co
- 8 play[.]googleapis[.]com
- 8 e673[.]dsce9[.]akamaiedge[.]net

Information on Insecure HTTP Requests

The device communicates without encryption (plain HTTP) with several websites. Each connection that is not encrypted (uses HTTP instead of HTTPS), transfers information that potentially anyone with access to the device traffic can see without major effort. Who can access the traffic? This is illustrated by the Electronic Frontier Foundation at https://www.eff.org/pages/tor-and-https. People that share your WiFi, internet service providers, mobile cellular networks, and others. For maximum privacy, it's better if all connections from the phone are encrypted. If you are a person at risk, we recommend uninstalling all applications that are not essential. Use a VPN when using public and not trusted networks.

List of websites visited using HTTP:

- www[.]berlineastsidegalleryfilm[.]de (2 requests)
- connectivitycheck[.]gstatic[.]com (2 requests)
- ocsp[.]pki[.]goog (1 requests)
- proxy-safebrowsing[.]googleapis[.]com (1 requests)

Every HTTP connection has many pieces of data, among them the User-Agent. User-Agents identify the device and application so the content is properly shown on the mobile phone. We automatically analyze the User-Agents observed in the insecure connections listed above and automatically extract information that can identify the application and device:

- Mozilla/5.0 (iPhone; CPU iPhone OS 14_7_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.2 Mobile/15E148 Safari/604.1
  - Information extracted: iPhone / iOS 14.7.1 / Mobile Safari 14.1.2
- Twitter/8.75.1 CFNetwork/1240.0.4 Darwin/20.6.0
  - Information extracted: iOS-Device / iOS / Twitter 8.75.1
- com.apple.trustd/2.1
  - Information extracted: Other / Other / Other
- SafariSafeBrowsing/16611.3.10.0.1 CFNetwork/1240.0.4 Darwin/20.6.0
  - Information extracted: iOS-Device / iOS / CFNetwork 1240.0.4