Hummer Trojan - Indicators of Compromise

Foreign Connections Established by Hummer Trojan from the Device

Remote IP	Remote Port	Package:UID	Last Seen	Activity(sec.)
96.17.202.209	80	com.hd.android.tubede:10077	7/6/16 15:29	212
23.23.156.83	80	com.hd.android.tubede:10077	7/6/16 15:22	10
185.32.28.190	80	com.hd.android.tubede:10077	7/6/16 15:22	10
52.8.103.19	80	com.hd.android.tubede:10077	7/6/16 15:22	16
52.73.84.217	80	com.hd.android.tubede:10077	7/6/16 15:24	46
52.200.29.247	443	com.hd.android.tubede:10077	7/6/16 15:22	6
52.3.205.231	443	com.hd.android.tubede:10077	7/6/16 15:25	20
54.209.75.249	443	com.hd.android.tubede:10077	7/6/16 15:22	12
54.251.182.28	80	com.hd.android.tubede:10077	7/6/16 15:22	10
54.225.236.108	80	com.hd.android.tubede:10077	7/6/16 15:22	8
216.223.26.160	80	com.hd.android.tubede:10077	7/6/16 15:24	28
52.202.47.159	443	com.hd.android.tubede:10077	7/6/16 15:25	12
199.83.134.214	80	com.hd.android.tubede:10077	7/6/16 15:28	170
54.230.6.151	80	com.hd.android.tubede:10077	7/6/16 15:24	40
104.250.133.114	80	com.hd.android.tubede:10077	7/6/16 15:37	544
54.169.219.69	8081	com.hd.android.tubede:10077	7/6/16 15:22	12
139.162.61.40	8080	com.hd.android.tubede:10077	7/6/16 15:22	4
54.186.5.53	7017	com.hd.android.tubede:10077	7/6/16 15:33	288
139.162.28.46	8080	com.hd.android.tubede:10077	7/6/16 15:22	4
45.33.120.75	80	com.hd.android.tubede:10077	7/6/16 15:22	4
52.40.93.66	7017	com.hd.android.tubede:10077	7/6/16 15:29	200
54.222.175.197	443	com.hd.android.tubede:10077	7/6/16 15:24	4
162.221.12.172	80	com.hd.android.tubede:10077	7/6/16 15:37	44
45.33.0.176	80	com.hd.android.tubede:10077	7/6/16 15:24	4
45.79.177.230	80	com.hd.android.tubede:10077	7/6/16 15:30	256

128.199.193.15	80	com.hd.android.tubede:10077	7/6/16 15:37	282
23.23.103.84	80	com.hd.android.tubede:10077	7/6/16 15:25	22
178.162.219.54	80	com.hd.android.tubede:10077	7/6/16 15:24	16
75.101.138.48	80	com.hd.android.tubede:10077	7/6/16 15:25	22
52.76.99.19	32090	com.hd.android.tubede:10077	7/6/16 15:31	8
52.40.93.66	7012	com.hd.android.tubede:10077	7/6/16 15:24	2
52.24.14.90	7011	com.hd.android.tubede:10077	7/6/16 15:24	2
52.34.189.89	10091	com.hd.android.tubede:10077	7/6/16 15:30	208
52.71.66.56	443	com.hd.android.tubede:10077	7/6/16 15:25	18
173.1.1.168	80	com.hd.android.tubede:10077	7/6/16 15:24	10
173.1.1.163	80	com.hd.android.tubede:10077	7/6/16 15:26	64
54.235.150.30	443	com.hd.android.tubede:10077	7/6/16 15:25	14
52.20.239.155	443	com.hd.android.tubede:10077	7/6/16 15:25	14
108.166.13.14	80	com.hd.android.tubede:10077	7/6/16 15:27	92
54.197.254.235	80	com.hd.android.tubede:10077	7/6/16 15:25	12
52.74.57.9	80	com.hd.android.tubede:10077	7/6/16 15:24	2
52.74.106.19	80	com.hd.android.tubede:10077	7/6/16 15:30	268
104.31.70.143	80	com.hd.android.tubede:10077	7/6/16 15:30	268
104.31.92.178	80	com.hd.android.tubede:10077	7/6/16 15:37	90
54.230.6.78	80	com.hd.android.tubede:10077	7/6/16 15:27	52
216.121.96.28	80	com.hd.android.tubede:10077	7/6/16 15:30	202
52.74.133.116	80	com.hd.android.tubede:10077	7/6/16 15:26	2
216.58.194.78	80	com.hd.android.tubede:10077	7/6/16 15:30	150
216.58.194.78	443	com.hd.android.tubede:10077	7/6/16 15:30	300
172.217.1.162	443	com.hd.android.tubede:10077	7/6/16 15:30	150
216.58.195.34	443	com.hd.android.tubede:10077	7/6/16 15:33	214
54.222.158.91	80	com.hd.android.tubede:10077	7/6/16 15:30	150
54.223.82.182	80	com.hd.android.tubede:10077	7/6/16 15:30	150
128.199.254.160	80	com.hd.android.tubede:10077	7/6/16 15:30	90
216.58.194.110	443	com.hd.android.tubede:10077	7/6/16 15:36	942

216.58.218.162	443	com.hd.android.tubede:10077	7/6/16 15:33	64
54.222.183.235	443	com.hd.android.tubede:10077	7/6/16 15:31	6
54.222.182.197	80	com.hd.android.tubede:10077	7/6/16 15:31	6
54.230.6.167	80	com.hd.android.tubede:10077	7/6/16 15:33	58
218.213.248.174	80	com.hd.android.tubede:10077	7/6/16 15:33	116
107.21.255.237	80	com.hd.android.tubede:10077	7/6/16 15:33	116
54.229.132.190	443	com.hd.android.tubede:10077	7/6/16 15:33	116
96.17.202.177	80	com.hd.android.tubede:10077	7/6/16 15:36	302
54.86.227.192	443	com.hd.android.tubede:10077	7/6/16 15:33	116
192.230.66.214	80	com.hd.android.tubede:10077	7/6/16 15:36	244
45.79.93.81	80	com.hd.android.tubede:10077	7/6/16 15:37	62
52.74.103.78	7077	com.hd.android.tubede:10077	7/6/16 15:37	62
52.6.207.177	443	com.hd.android.tubede:10077	7/6/16 15:36	372
52.77.99.53	80	com.hd.android.tubede:10077	7/6/16 15:36	186
54.223.81.2	80	com.hd.android.tubede:10077	7/6/16 15:37	4
104.31.71.143	80	com.hd.android.tubede:10077	7/6/16 15:37	4

List of IPs and Domains that the Malicious App communicates with

- 173.1.1.163
- 45.33.120.75
- 45.79.140.33
- 45.79.146.48
- 45.79.177.230
- 45.79.180.126
- 45.79.77.161
- 52.76.99.19
- 54.169.219.69
- a.asense.in
- active.WKSNKYS7.COM
- ad.adspoo.com
- adm.kemoge.net
- ads.glispa.com
- alog.umeng.c
- alog.umeng.com
- api.ddongfg.com
- api.gadmobs.com
- api.holawords.com
- api.meetcakes.com
- apkcar.com
- apk.cs9adv.com
- app.adjust.io

- app.king7r.com
- c.afftrx.com
- cler.zjlnjx.com
- clk.taptica.com
- d1qxrv0ap6yf2e.cloudfront.net
- d1us587r5hte4i.cloudfront.net
- d2h8j6qo1tr30c.cloudfront.net
- d37vptlvrx6hxq.cloudfront.net
- d795nz9qqyd60.cloudfront.net
- d.amobicdn.com
- dd.truckskyfly.com
- down.akocdn.com
- down.amobitrack.com
- down.upgamecdn.com
- ecget.hmapi.com
- ecget.yhmapi.com
- ecget.yikuaizuan.cc
- ecreport.hmapi.com
- ecreport.Leoquan.cc
- ecreport.yhmapi.com
- ecupdate.yhmapi.com
- efget.yhmapi.com
- eiget.yhmapi.com
- epcontrol.yhmapi.com
- epget.Leoquan.cc
- epreport.Leoquan.cc
- epupdate.yhmapi.com
- fget.guangbom.com
- gapi.iwhalenews.com
- gp.like383.com
- gp.miaoxia123.com
- gyd.poo268.com
- hgupdate.eoapi.com
- hgupdate.hmapi.com
- id1.cn
- inf.amz.uyfit.com
- interface1.kokmobi.com
- interface.234vs.com
- interface.kokmobi.com
- interface.madpush.com
- ipinfo.io
- k.sonyba.com
- log.appsolo.net
- log.ddongfg.com
- m.AEDXDRCB.COM
- mas.goaapis.com
- masmonty.com
- m.iwhalenews.com
- m.xmobitrack.com
- oc.umeng.com
- ph1.99youx.com
- ph2.99youx.com
- ph3.99youx.com
- ph3.buydudu.com
- ph4.99youx.com
- ppsdk.yhmapi.com
- res.rayjump.com

- rp.uyfit.com
- 103136.api-02.com
- 158236.measurementapi.com
- 167394.measurementapi.com
- 17900.measurementapi.com
- s2s.exloadlinks.com
- 75032.measurementapi.com
- 81458.measurementapi.com
- admin.appnext.com
- sdk.mobnativeads.com
- service.sm-adoss.com
- go.mobra.in
- mqdownloads.s3.amazonaws.com
- odr.mookie1.com
- t.mobitrk.com
- sys.aedxdrcb.com
- yt3.ggpht.com
- tdcv3.talkingdata.net
- tongji.adspoo.com
- track.56txs4.com
- tracking.adactioninteractive.com
- tracking.adkmob.com
- tracking.lenzmx.com
- traktum.com
- trans.mobimax.info
- trk.glispa.com
- u.amobisc.com
- up.appsolo.net
- verify.iposdk.com
- ws.sd4face.com
- apxadtracking.net
- kalazz.com
- ohnowhathappened.com
- sm-adoss.com
- startappexchange.com
- venturead.com
- weemobi.com
- woomobi.com
- xtra1.gpsonextra.net
- xtra3.gpsonextra.net
- ymex.apkcar.com
- ymlog.apkcar.com
- ymsdk.apkcar.com

URLs for the APKs downloaded on the device

- http://apk.cs9adv.com/upload/plug-ins/CCleann201607041.apk
- http://apk.cs9adv.com/upload/root/com.system.update800031.apk
- http://app.king7r.com/upload/attachment/20160530/20160530163502547.apk
- http://d795nz9qqyd60.cloudfront.net/upload/ssp/1466070267899.apk
- http://d.amobicdn.com/the_marlboro/icon20160123.apk
- http://down.akocdn.com/onemain/maink.apk
- http://down.akocdn.com/onemain/mains2.apk
- http://down.amobitrack.com/backokr/rtt_0310_577.apk
- http://res.rayjump.com/common/2016/06/15/16/35/14659798205924.apk
- http://res.rayjump.com/common/2016/06/15/16/36/14659798513256.apk

- http://rp.uyfit.com/superboost_289.001.007.apk
- https://mqdownloads.s3.amazonaws.com/173b0c8b0aa26731f70d4926c1479fad/BestWallpaper-0623DDL_20160623_ddl-avazu-w-a.apk