Vetting Malicious Android Apps

Rohith Mulumudy

January 14, 2024

1 Compass App

APK link: com.lu.compass

The app is making the following API calls:

1. `http://www.umeng.co`
2. `http://www.umeng.com`
3. `http://ad.leadboltapps.net`
4. `https://api.airpush.com`
5. `http://cp.pushwoosh.com`

The parameters for the above APIs:

1. `http://www.umeng.co/check_config_update`
2. `http://www.umeng.com/check_config_update`
3. `http://www.umeng.com/api/check_app_update`
4. `http://www.umeng.com/app_logs`
5. `http://ad.leadboltapps.net/optin?&section_id=648709860&mode=0`
6. `http://ad.leadboltapps.net/optin?&section_id=687484172&mode=0`
7. `https://api.airpush.com/v2/api.php`
8. `https://api.airpush.com/lp/log_sdk_request.php`
9. `https://api.airpush.com/newad/report/logUserBrowserHistory.php`
10. `http://cp.pushwoosh.com/json/1.3/applicationOpen`
11. `http://cp.pushwoosh.com/json/1.3/registerDevice`

2 Youtube video downloader

APK link: com.ddev.downloader.v2

The app is making the following API calls:

1. `http://ad.leadboltapps.net`
2. `https://android.bcfads.com`
3. `http://www.apperhand.com`
4. `http://www.droidsettings.com`
5. `http://www.uk-droidsettings.com`
6. `https://api.airpush.com`
7. `https://www.youtube.com`

The parameters for the above APIs:

1. `http://ad.leadboltapps.net/show_app.conf?&get=SXZvWDgzZlVWN0E5QndqVBwTEYURgE7HjpL`
   `HFS86gFD336-6Pv2cXnN3y5JoiStdTPw~~&section_id=530725215`
2. `http://ad.leadboltapps.net/show_notification?&get=UXJQQ1c5QVE3dTVXOUxmapEfWJ_`
   `GISVNwXD12P0tR4wAZJhuAiYXvQy0R7F363PjLaBT908-YQq1MuxJfmyq8IQYbUbfoazznQhBlTA6AGuC`
   `ERx5KmTueGDFwnqgtwv6NoKNeARPwg8GOegEg~~&section_id=572647455`
3. `https://android.bcfads.com/api/v4/mobile_apps/5009f17dad9e62000c00000e/fullscreens/fetch.json`
4. `https://android.bcfads.com/api/v4/mobile_apps/5009f17dad9e62000c00000e/pop_ups/fetch.json`
5. `http://www.apperhand.com/ProtocolGW/protocol/commands`
6. `http://www.droidsettings.com/apps/tubemate8.json`
7. `http://www.uk-droidsettings.com/apps/tubemate8.json`
8. `https://api.airpush.com/v2/api.php`
9. `https://www.youtube.com/s/search/audio/failure.mp3`
10. `https://www.youtube.com/s/search/audio/no_input.mp3`
11. `https://www.youtube.com/s/search/audio/success.mp3`
12. `https://www.youtube.com/s/search/audio/open.mp3`