

**Nagra Anti-
Piracy Services
(Public version)
August 2021**

Executive Summary

The objective of this project is to (i) identify the most impactful free and paid Apps used to illegally distribute content and channel of Alianza member, (ii) remove such Apps from App Stores to prevent new user from using them, (iii) takedown infringing playlists used by such Apps to prevent users who have already installed such Apps from using the Apps.

The analysis of potential pirate Apps and Playlists was performed in the main App Stores and sharing sites available on the Internet. The Apps and Playlists were searched using specific keywords to detect candidates for analysis.

Principal Findings

The August 2021 Pirate Apps & Lists Detection and Removal Alliance Project Monthly Report highlights the following:

- **148 unique pirated Apps** were removed from the platforms, with 69 of them being free Apps and 79 being paid Apps.
 - A total of 30 Apps were removed from the Google Play platform, 62 Apps were removed from the APK Combo platform, 45 Apps were removed from the DownloadAPK platform, 8 Apps were removed from the Aptoide platform, and 3 Apps were removed from the APK Pure platform in August 2021.
- **269 free Playlists** were removed from the different platforms on the Internet.
 - In these Playlists that were removed there were a total of 33,333 streaming violations (TV channels, movies or TV series of Alianza members participating in the program) that were redistributed without authorization.
- Total number of pirated Apps and Playlists removed since the start of the program on July 1, 2019: **915 Apps and 9,457 Playlists**. The following is an example.

Annex I – Project Scope Definition

This section briefly describes the scope of the App Detection Project for the audience comprehension.

Free-to-access- The goal is to identify **free**, widely available and often highly visible pirate services distributed through mobile applications (“Apps”), and M3U Lists (“Playlists”). This type of piracy is usually of variable quality and reliability and plagued by advertisements and malware.

Automatic Crawling (Scan) – NAGRA employs an automatic crawling tool which performs searches in the most popular application market stores available on the Internet such as:

- Google Play: <https://play.google.com/store/apps>
- Apple Store: <https://www.apple.com/ae/ios/app-store/>
- APK Monk: <https://www.apkmonk.com/>
- Aptoide: <https://en.aptoide.com/>
- DownloadAPK: <https://downloadapk.net/>

The searches are performed **twice a month** in the stores using specific search terms (keywords) related to the ALIANZA members chosen to maximize the number of Apps & Playlists found.

Classification - Once the Apps or Playlists are found, they are automatically classified using NAGRA’s extensive and ever-increasing database of reviewed Apps to determine if it is free, paid, pirate, non-pirate, white-listed, etc.

In the case of Apps, if they happen to be new to the database, NAGRA installs the Apps on compatible devices to test the content and channels made available and registers the type accordingly. Additionally, NAGRA analyzes the network traffic of the Apps classified as Pirate, to track down the hosts of the pirated content.

For Playlists, all new entries are downloaded and reproduced on a compatible player to perform the same analysis as the one done in Apps.

Takedown of Pirate Apps and Playlists - Once the pirate Apps and Playlists are identified, evidence is gathered, and the takedown process is triggered.

Abuse notifications are sent to the platforms hosting or promoting the pirate Apps and

Playlists. The notifications are issued following each particular platform's guidelines.

After the abuse notifications are issued, NAGRA performs an automatic follow up of the targets. Once the App or Playlist is detected as unavailable, the effective takedown is registered in the database to be reflected in the report.

Report - The data collected during the scanning, the classification process, as well as the evidence and takedown information will be presented in a monthly report. The report will contain analysis on the number of items found for both bi-weekly scans in the corresponding period along with results of the takedown notices.

Annex II - Terminologies Used

This section is to present to the audience the meaning of the terms used in this report.

Search Campaign (Scan) – The process of searching and identifying Apps and Playlists that advertise ALIANZA member’s content and channels. The search is based on keywords and is done twice a month (bi-weekly).

Classification (filtering) – Step that eliminates false positives, duplicates, Apps that were already tagged as Pirate, Non-Pirate, White-Listed Apps.

Review – The manual process of downloading, installing and classifying the App.

App – An app is a computer program which can be installed in a mobile device. Apps can have different purposes such as information/news access, social networking, playing games, multimedia, etc. They are distributed in the official App Stores for their respective mobile operating systems and in alternative stores.

Pirate App – Mobile applications that are, after review, confirmed to be making available ALIANZA member’s content or channels without proper authorization.

Non-Pirate - App or Playlist that is after review confirmed to carry other type of content or channels that is not from ALIANZA members or no content at all. Pirate apps that do not make available content or channels of ALIANZA members are not considered as “Pirate” under this project.

White-List – List of Apps and Playlists that were previously confirmed by ALIANZA members to be legitimate and therefore authorized to transmit content or channels, or that ALIANZA members do not wish to be taken down for the moment due to on-going investigations.