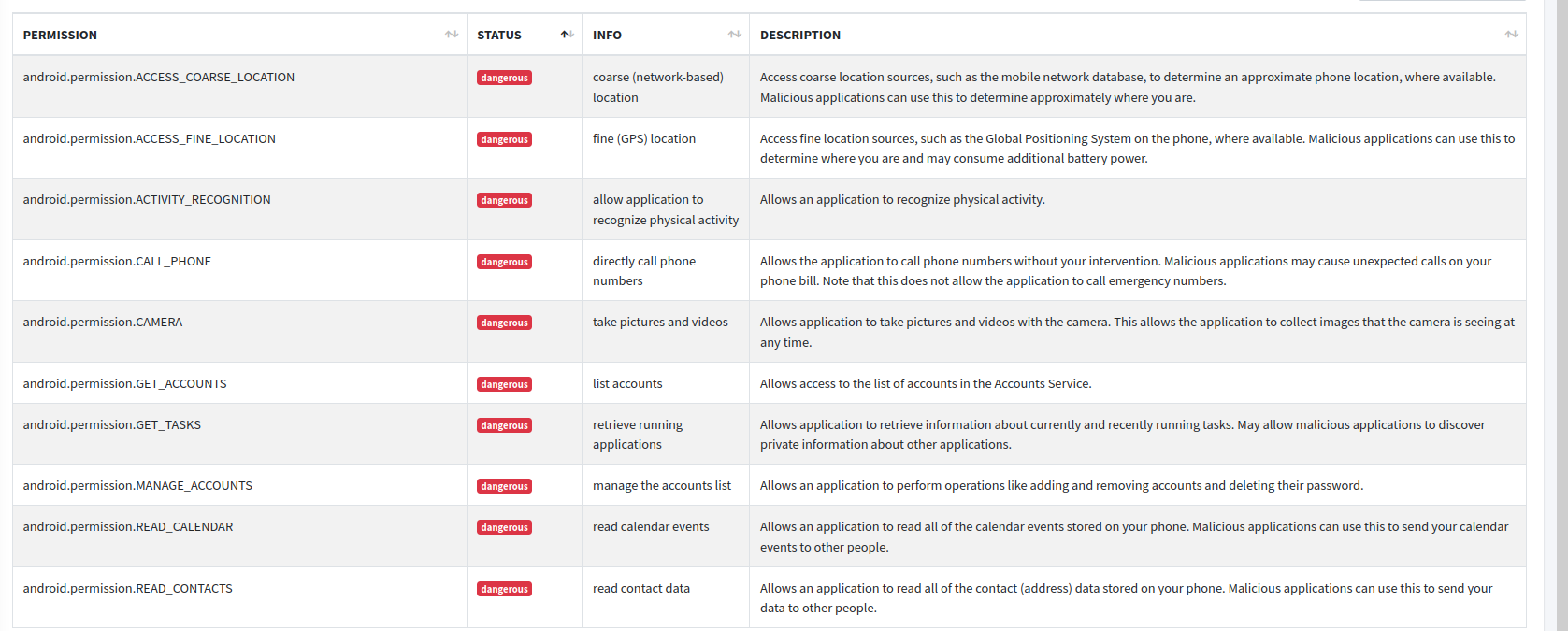
Chọn 2 ứng dụng Android cùng một công ty phát triển, hãy phân tích:

* Ở đây em chọn file Google\_14.17.36.29.arm64\_Apkpure.apk và file YouTube\_18.18.36\_Apkpure.apk đều của cùng công ty của google
* Để phân tích ta chọn mobsf
* Google



* Đây là các permission mà được cho là nguy hiểm
* Ta có thể thấy là có 1 số permission có quyền truy cập vào dữ liệu của điện thoại để xác định vị trí, lấy thông tin danh bạ, xem các tài khoản trong điện thoại và cũng có quyền thêm xóa hoặc sửa các tài khoản đó



* Đây là các thông tin về custom permission do ứng dụng tạo ra
* Custom permission:

+ com.google.android.voicesearch.AUDIO\_FILE\_ACCESS: cho phép truy cập vào các tệp âm thanh được tạo bởi ứng dụng Google Voice Search.

+ com.google.android.apps.now.CURRENT\_ACCOUNT\_ACCESS: cho phép truy cập vào tài khoản Google hiện tại trên thiết bị.

+ com.google.android.googlequicksearchbox.LAUNCH\_WITH\_RECORDED\_AUDIO: cho phép ứng dụng Google Quick Search Box khởi chạy với âm thanh đã ghi âm.

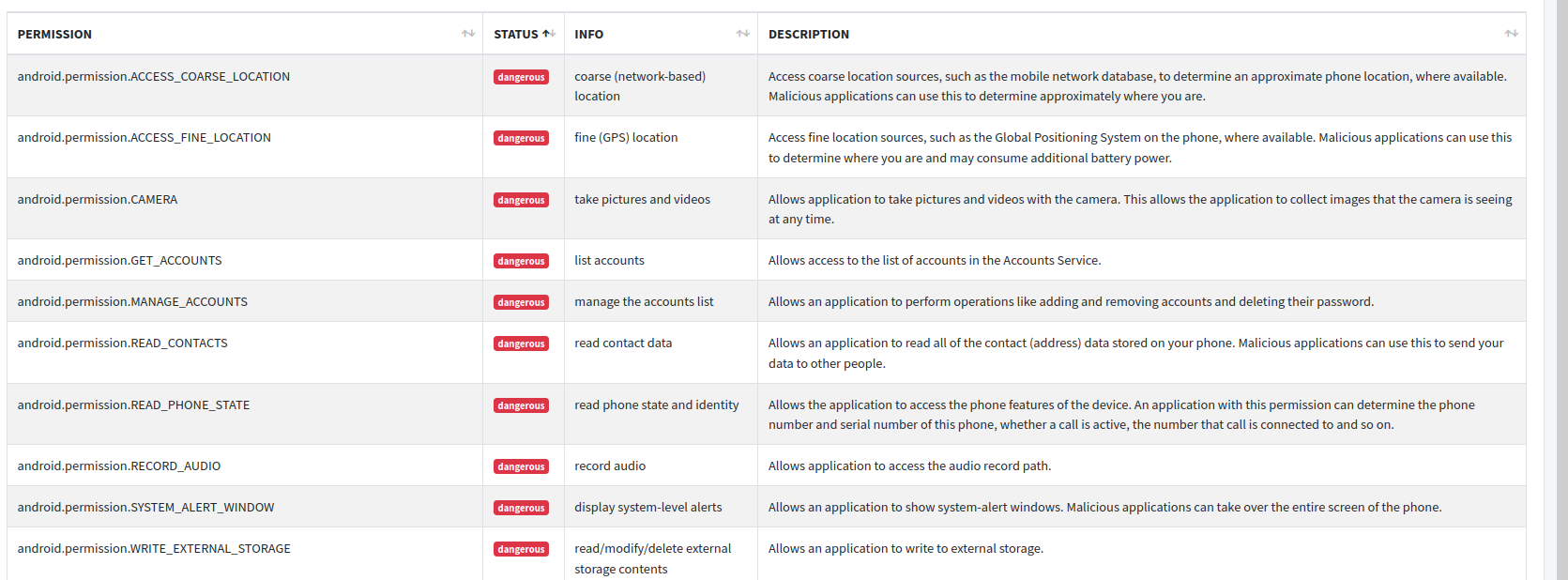
+ com.google.android.googlequicksearchbox.LAUNCH\_FROM\_DSP\_HOTWORD: cho phép ứng dụng Google Quick Search Box khởi chạy từ hotword DSP.

+ com.google.android.googlequicksearchbox.permission.PAUSE\_HOTWORD: cho phép ứng dụng Google Quick Search Box tạm dừng hotword DSP.

Ảnh có chứa văn bản, ảnh chụp màn hình, tài liệu, đại số

Mô tả được tạo tự động

* Đây là thông tin về chữ ký của ứng dụng
* Cho thấy là nó đã được ký bởi google và có tới 3 chữ ký khác nhau
* Thông tin về chứng chỉ cũng được cung cấp, cho thấy rằng chứng chỉ này thuộc về Google và có thời hạn từ năm 2008 đến năm 2036. Ngoài ra, các giá trị băm (hash) của APK cũng được cung cấp, bao gồm các giá trị băm MD5, SHA-1, SHA-256 và SHA-512, cùng với thông tin về thuật toán mã hóa và độ dài khóa công khai.
* Youtube



* Đây là các permission trong ứng dụng youtube, ta thấy nó cũng khá tương tự như google
* ứng dụng cũng có các quyền để ghi vào bộ nhớ của thiết bị. Đây có thể là tiền để để các attacker nhúng virus hoặc trojan vào video sao đó khi ta click vào thì ta vô tình tải chúng về
* Custom permission

+ com.google.android.youtube.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION: Đây là một quyền tùy chỉnh được tạo ra bởi ứng dụng YouTube để đảm bảo rằng chỉ các ứng dụng được phát triển bởi cùng một nhà phát triển (Google) mới có thể truy cập vào một phần của ứng dụng YouTube. Quyền này được bảo vệ bằng chữ ký và chỉ có thể được sử dụng bởi các ứng dụng khác được phát triển bởi Google.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

* Đây là thông tin signature của ứng dụng
* Thông tin trên cho biết rằng tệp APK này đã được ký với v2 signature và v3 signature, nhưng không ký với v1 signature. Chứng chỉ duy nhất được tìm thấy được phát hành bởi Google, có hiệu lực từ ngày 02/12/2008 đến ngày 19/04/2036, và có thuật toán chữ ký là rsa. Chứng chỉ này có độ dài khóa là 1024 bit và được đánh dấu bằng một fingerprint.