Malware Analysis

August 27, 2022

1 Permissions

1.1 .\resultados\diff_techbigs_badoo.json

Added Permissions
No added permissions

1.2 .\resultados\diff_techbigs_disney.json

Added Permissions
'android.permission.WRITE_EXTERNAL_STORAGE'
'android.permission.BLUETOOTH_ADMIN'
'android.permission.READ_EXTERNAL_STORAGE'
'net.dinglisch.android.tasker.PERMISSION_RUN_TASKS'
'android.permission.BLUETOOTH'
'android.permission.FLASHLIGHT'
'android.permission.WRITE_SETTINGS'
'android.permission.CHANGE_WIFI_STATE'
'android.permission.CAMERA'
'android.permission.VIBRATE'
'android.permission.ACCESS_WIFI_STATE'
'android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS'
'android.permission.READ_SETTINGS'
'android.permission.READ_LOGS'
'android.permission.SYSTEM_ALERT_WINDOW'

1.3 .\resultados\diff_techbigs_netflix.json

Added Permissions
'android.permission.VIBRATE'
'com.mozillaonline.downloads.com.teamseries.ACCESS_DOWNLOAD_MANAGER'
'android.permission.READ_EXTERNAL_STORAGE'
'android.permission.DOWNLOAD_WITHOUT_NOTIFICATION'
'android.permission.ACCESS_COARSE_LOCATION'
'com.mozillaonline.downloads.com.teamseries.SEND_DOWNLOAD_COMPLETED_INTENTS'
'android.permission.SYSTEM_ALERT_WINDOW'
'com.mozillaonline.downloads.com.teamseries.ACCESS_DOWNLOAD_MANAGER_ADVANCED'

Added Permissions
'com.google.android.providers.gsf.permisson.READ_GSERVICES'
'com.google.android.providers.gsf.permission.WRITE_GSERVICES'

2 Antivirus Scan

2.1 .\resultados\virustotal_techbigs_badoo.json

Antivirus	Virus founds
Trustlook	Android.PUA.DebugKey
ESET-NOD32	a variant of Android/Spy.Banker.BCS