14th Lab for Forensics

Rodrigo Castillo

16 de noviembre de 2020

1. Rules in Yara...

rule:i starting by creating the rule for yara, i created this rule because i found this string in my mp3 player... then , i proceed to check the rule in my mp3 player, so the result was

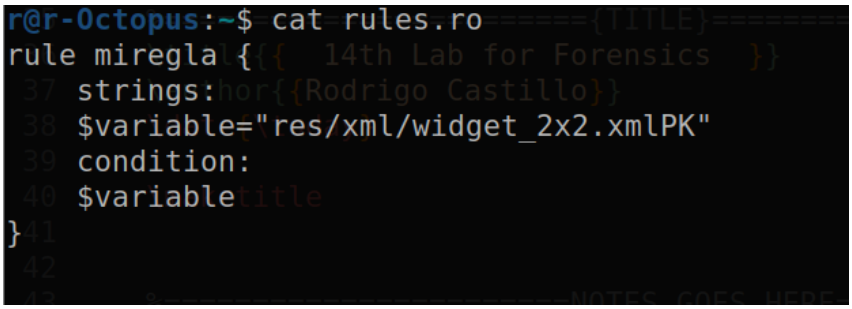

Figura 1: My Rule

this...

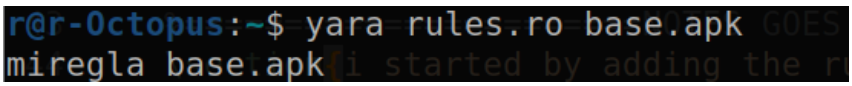

Figura 2: Rule detected on my mp3 player

2. malicious apk search

i started by adding the filters *detected* : *true* and *analyzed* : *true* to search for android malware with :

1. ilegal microtransactions
2. priviledge for spying the victim
3. priviledge for taking ilegal photos

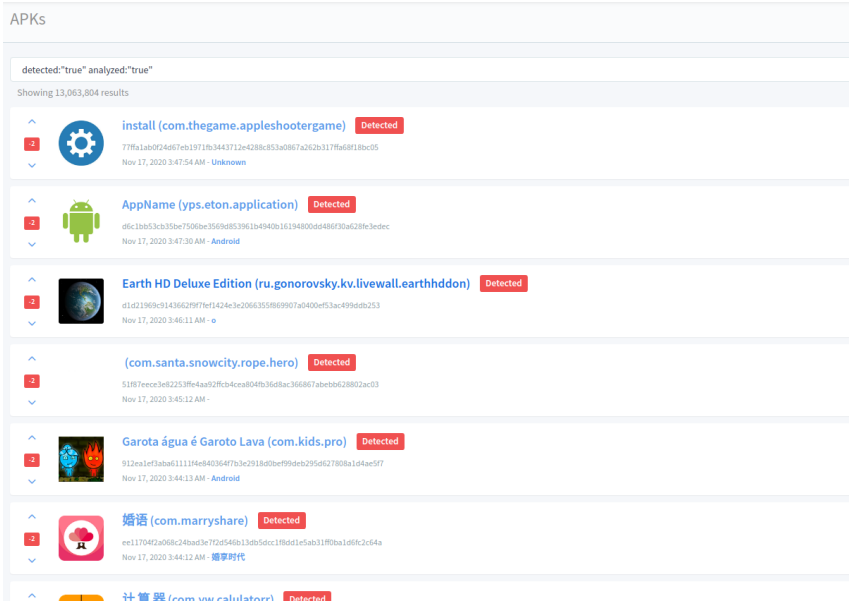

Figura 3: search

and what i found was....
1:application making illegal microtransactions via sms:
in **videox** we can see that is a reported application if we search for the analyst reports,

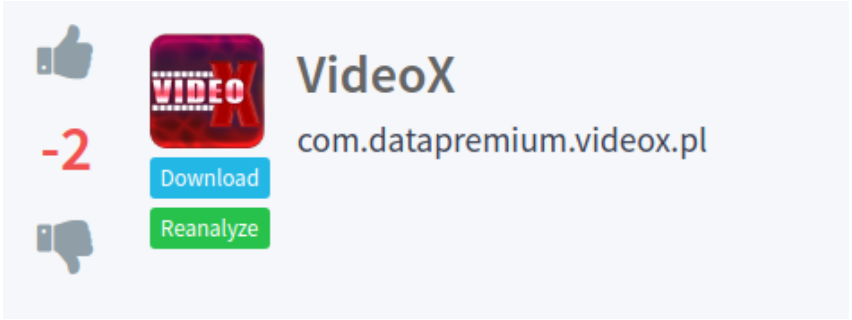

Figura 4: videox

we can see that the application has 20 permissions that is a lot, also, those permissions are related to sms control then, if we check for the sms functions, we can see that its calling an sms function this is a piece of malware that also takes advantages of other functionalities like phonecalls, but for the purpose of the lab i'm done.

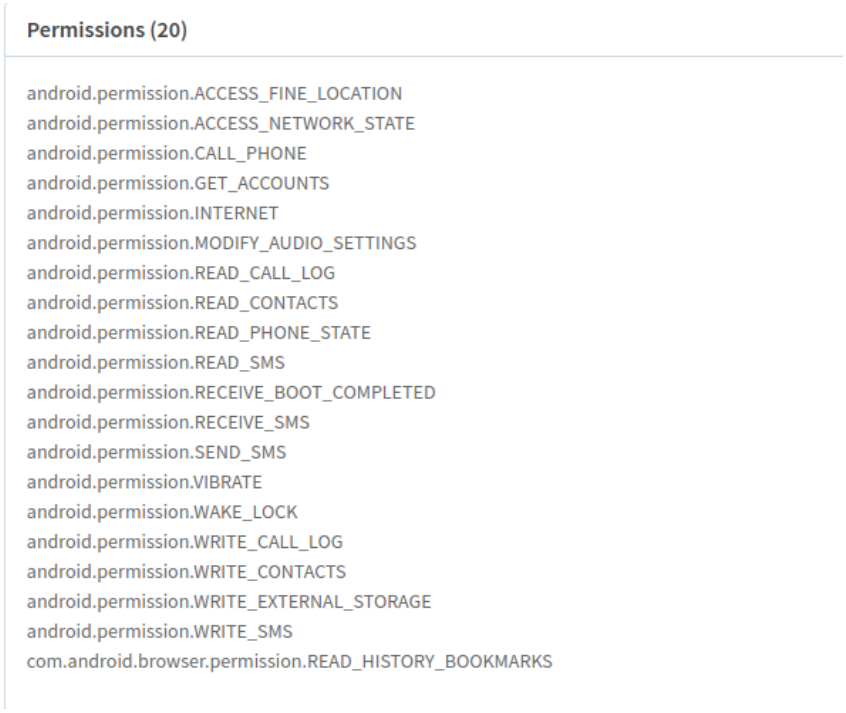

Figura 5: permissions of videox

Figura 6: sms

application for spying... this application is a piece of malware that has priviledges for spying the people who run it... we can notice that if we check the file permissions that

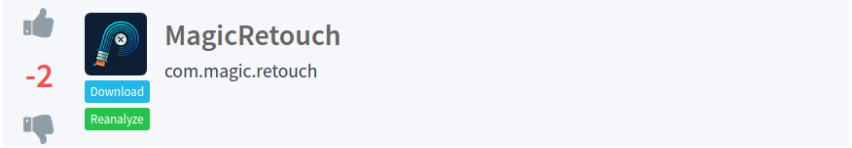

Figura 7: malware for spying

it requests...

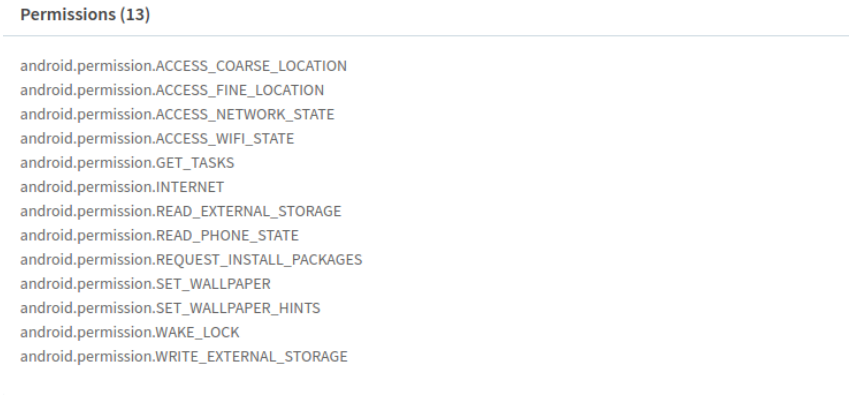

Figura 8: spy application permissions

application taking photos: i found this application that has the priviledge of taking photos with the camera of the cellphone. if we check for the permissions, it requiere privi-

Figura 9: application that takes photos

ledges for spying the victim... however, if we check for the function that the application its calling it is calling for cammera functions and its also taking both cammeras so its a piece of malware that is spying via camera

Permissions (23)

android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION
android.permission.ACCESS_NETWORK_STATE
android.permission.ACCESS_WIFI_STATE
android.permission.BATTERY_STATS
android.permission.BLUETOOTH
android.permission.GET_TASKS
android.permission.INTERNET
android.permission.MOUNT_UNMOUNT_FILESYSTEMS
android.permission.PACKAGE_USAGE_STATS
android.permission.READ_EXTERNAL_STORAGE
android.permission.READ_PHONE_STATE
android.permission.REAL_GET_TASKS
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.RECEIVE_USER_PRESENT
android.permission.SYSTEM_ALERT_WINDOW
android.permission.VIBRATE
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.WRITE_SETTINGS
com.android.launcher.permission.CREATE_SHORTCUT
com.android.launcher.permission.INSTALL_SHORTCUT
com.android.launcher.permission.UNINSTALL_SHORTCUT
com.asus.msa.SupplementaryDID.ACCESS

Figura 10: priviledges for spying

Functionalities - socket (3)

Functionalities - mcc (3)

Functionalities - crypto (3)

Functionalities - ssl (3)

Functionalities - camera (2)

Code	Class	Method
`invoke-virtual v0, Landroid/hardware/Camera;->startPreview()V`	Lcom/bx/bsdk/nnbs/MainActivity;	b
`invoke-virtual v2, Landroid/hardware/Camera;->startPreview()V`	Lcom/yanzhenjie/permission/a/f;	a

Functionalities - dynamicbroadcastreceiver (3)

Functionalities - imei (3)

Functionalities - iccid (3)

Functionalities - runbinary (3)

Functionalities - imsi (3)

Figura 11: cammera control