

# 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

```
r@r-Octopus:~$ cat rules.ro ====={||LE}=====
rule miregla{
  meta:
    14th Lab for Forensics
  strings:
    $variable="res/xml/widget_2x2.xmlPK"
  condition:
    $variabletitle
}
42
43
```

Figura 1: My Rule

this...

```
r@r-Octopus:~$ yara rules.ro base.apk GOES
miregla base.apk
```

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. illegal microtransactions
2. privilege for spying the victim
3. privilege for taking ilegal photos

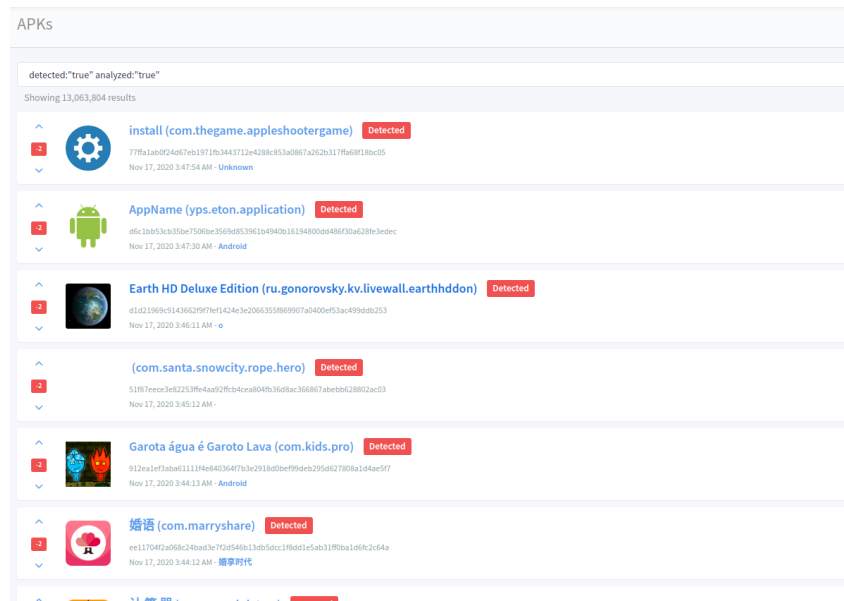


Figura 3: search

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,

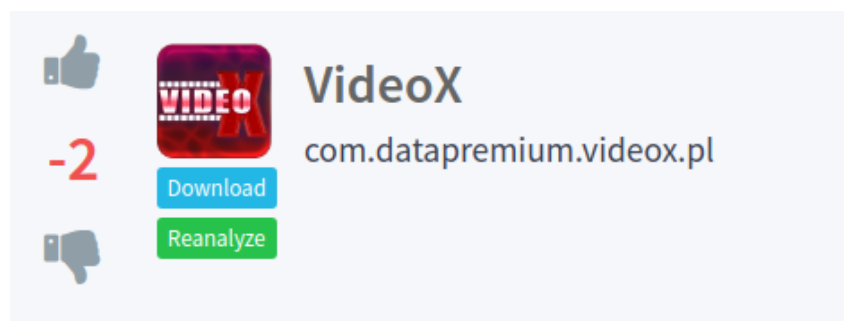


Figura 4: videox

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.

Permissions (20)
android.permission.ACCESS_FINE_LOCATION
android.permission.ACCESS_NETWORK_STATE
android.permission.CALL_PHONE
android.permission.GET_ACCOUNTS
android.permission.INTERNET
android.permission.MODIFY_AUDIO_SETTINGS
android.permission.READ_CALL_LOG
android.permission.READ_CONTACTS
android.permission.READ_PHONE_STATE
android.permission.READ_SMS
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.RECEIVE_SMS
android.permission.SEND_SMS
android.permission.VIBRATE
android.permission.WAKE_LOCK
android.permission.WRITE_CALL_LOG
android.permission.WRITE_CONTACTS
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.WRITE_SMS
com.android.browser.permission.READ_HISTORY_BOOKMARKS

Figura 5: permissions of videox

Functionalities - SMS (1)		
Code	Class	Method
invoke-virtual/range v0 ..., v5, Landroid/telephony/SmsManager;->sendTextMessage(Ljava/lang/String; Ljava/lang/String; Ljava/lang/String; Landroid/app/PendingIntent; Landroid/app/PendingIntent;)V	Lcom/datapremium/americanpayer/sms/SendSMS;	sendMsg

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

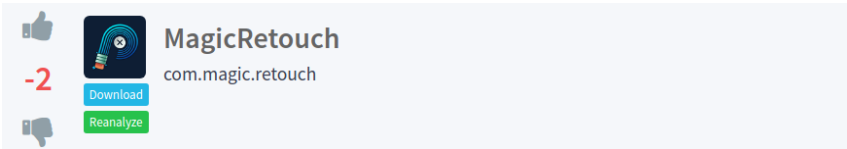


Figura 7: malware for spying

it requests...

#### Permissions (13)

```
android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION
android.permission.ACCESS_NETWORK_STATE
android.permission.ACCESS_WIFI_STATE
android.permission.GET_TASKS
android.permission.INTERNET
android.permission.READ_EXTERNAL_STORAGE
android.permission.READ_PHONE_STATE
android.permission.REQUEST_INSTALL_PACKAGES
android.permission.SET_WALLPAPER
android.permission.SET_WALLPAPER_HINTS
android.permission.WAKE_LOCK
android.permission.WRITE_EXTERNAL_STORAGE
```

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
<code>invoke-virtual v0, Landroid/hardware/Camera;.&gt;startPreview()V</code>	Lcom/bv/bsdk/nmb/MainActivity;	b
<code>invoke-virtual v2, Landroid/hardware/Camera;.&gt;startPreview()V</code>	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