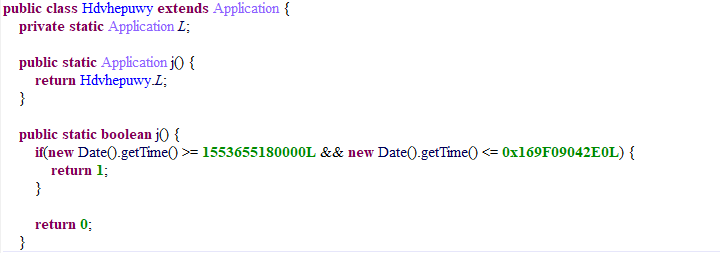
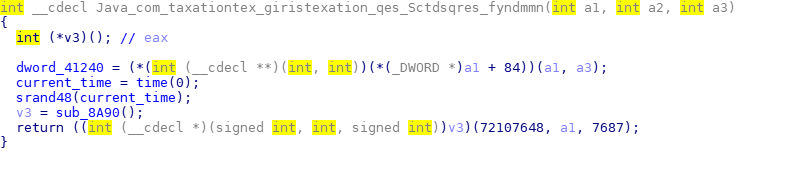
Android Malware Analysis : Dissecting Hydra Dropper

## Package name: om.taxationtex.giristexation

## Java Check time avoid sandbox:



## JNI Function:



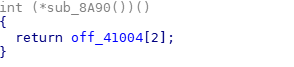
## Get the epoch time:



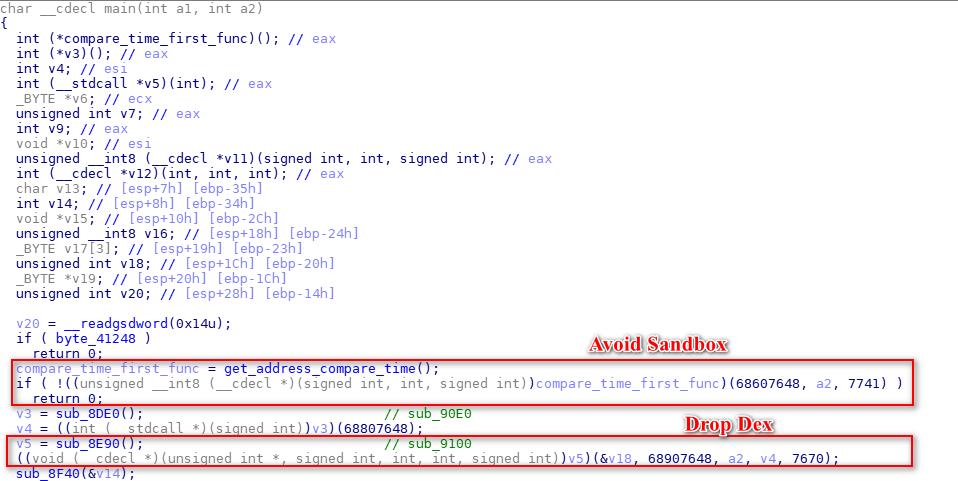
Current\_time< 1553655180 +0xD2F00 = 2019-04-06 10:53:00

Function Flow:

sub\_8A90()---> sub\_8B60()[rename main()]

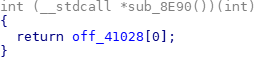
 

Avoid Sandbox & Drop Dex

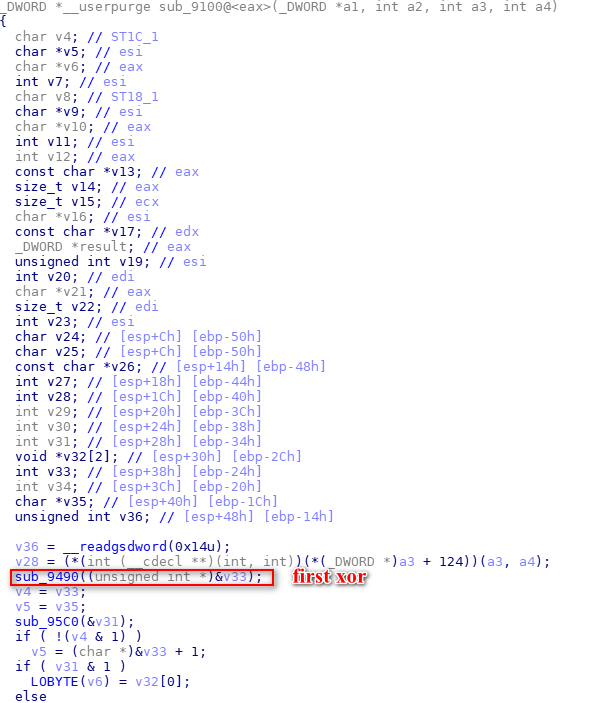


Drop Dex:

Main----> sub\_8E90()---->sub\_9100()

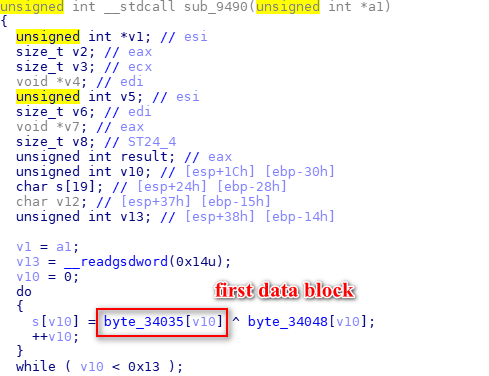
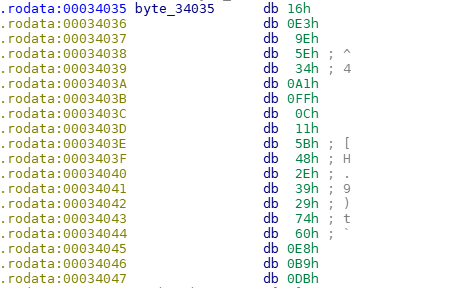
 

Sub\_9100()----> sub\_9490()

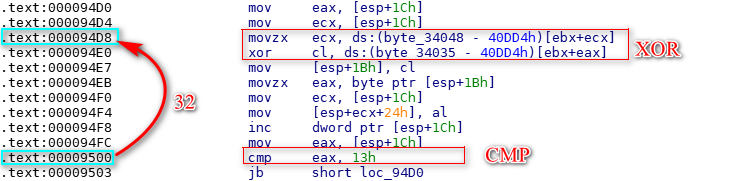


Sub\_9490()

Get first data block address: 0x00034035

Data\_block\_address\_xref+32 = cmp address <== block size

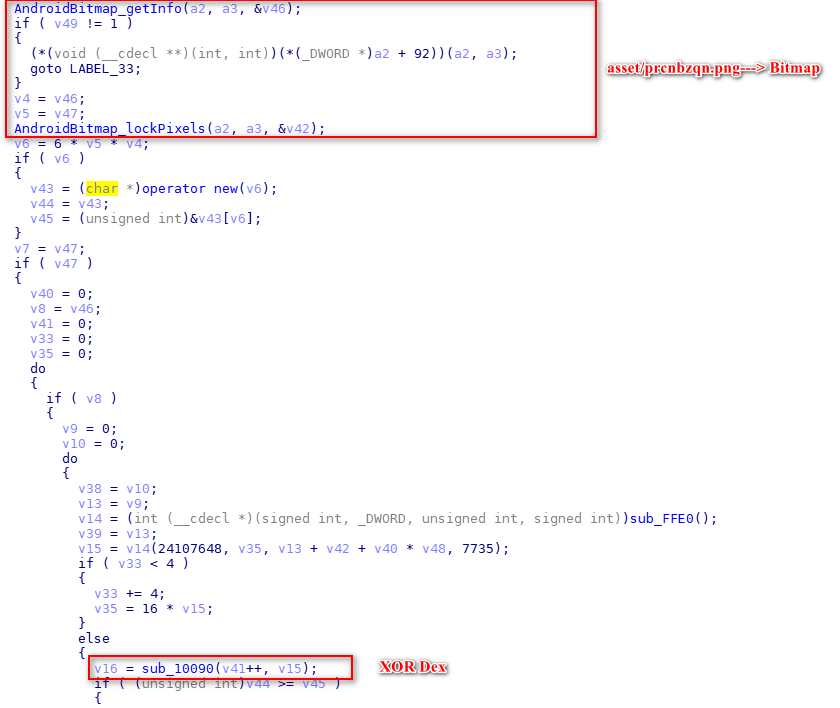
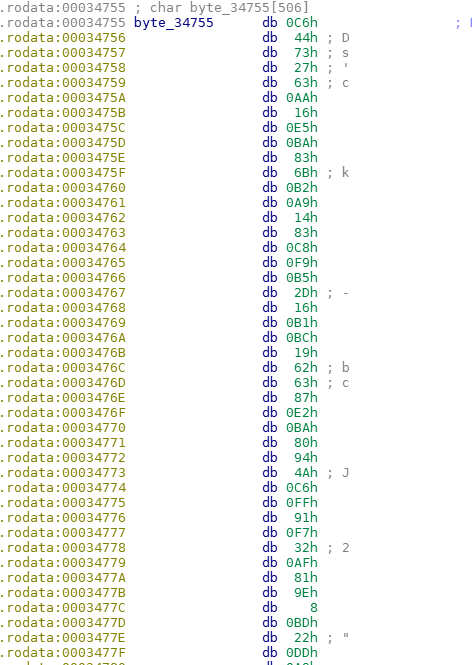


Pass XOR of DEX part:

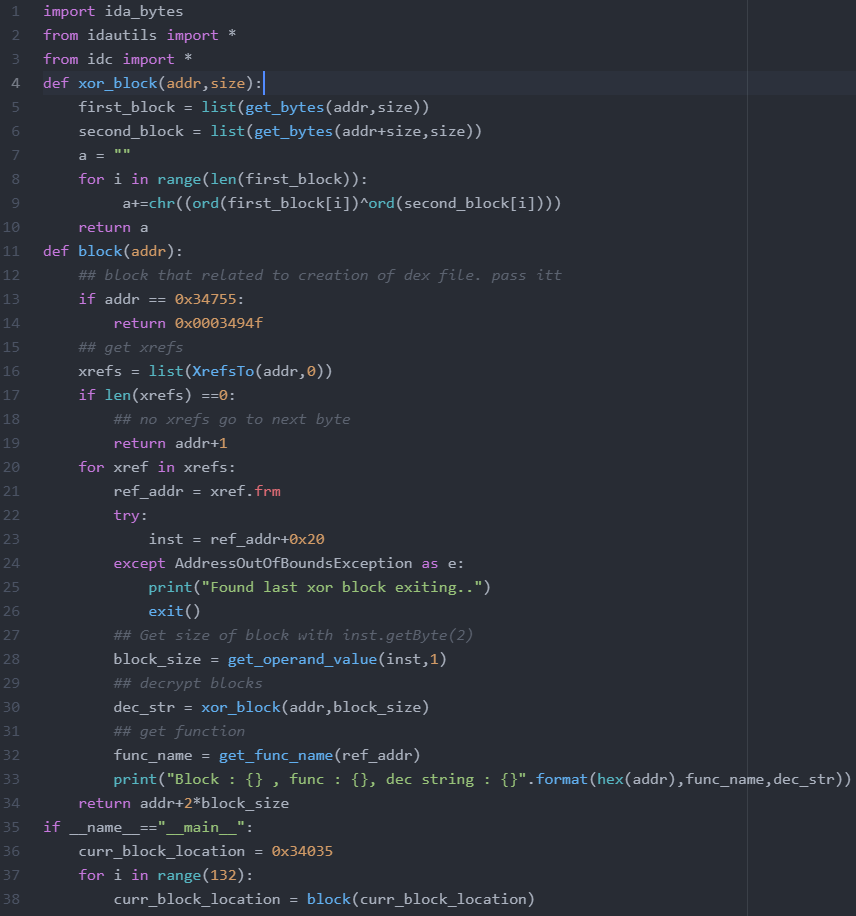
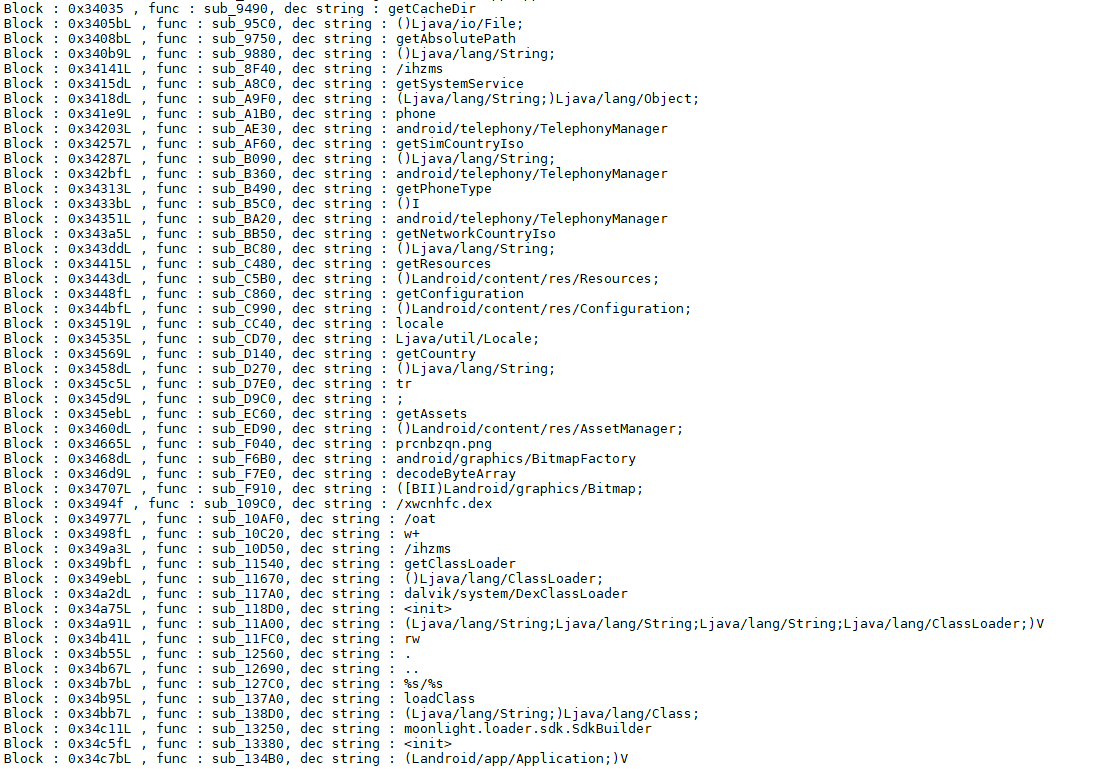
Main()---->sub\_9DA0()---->sub\_E2C0()---->sub\_E730()---->sub\_F2A0()---->sub\_F3D0()---->sub\_FBF0()---->sub\_10090()

0x34755+506=0x3494f

0x34755<=Dex Address<=0x3494f

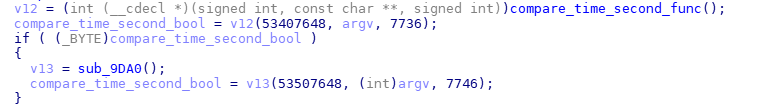
  

IDA Python Decry



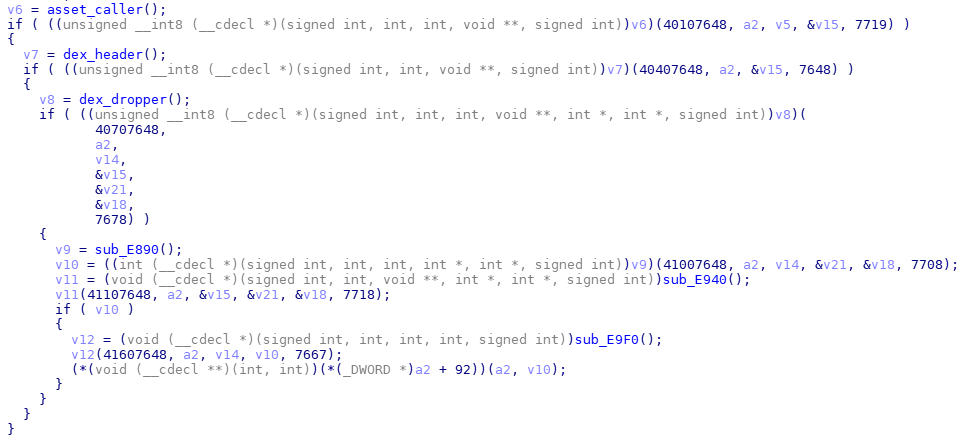
Second check time

Main()

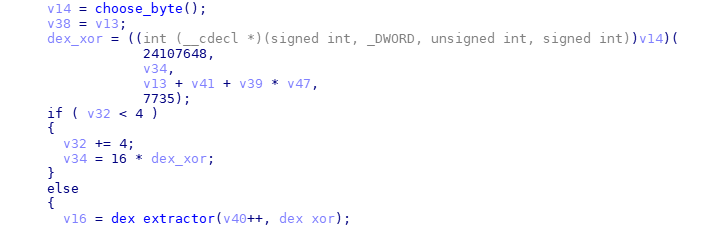
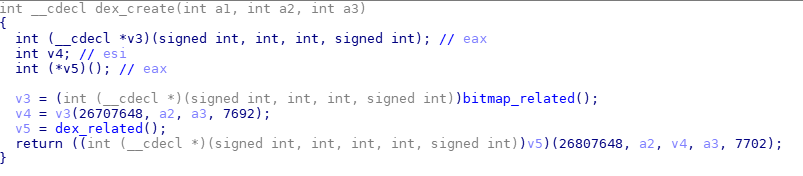


Drop Dex

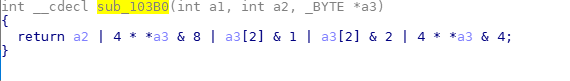
sub\_9DA0()------->off\_410DC[2]= sub\_E2C0()---->asset\_caller()[off\_41104()]-------->asset\_caller\_origin()



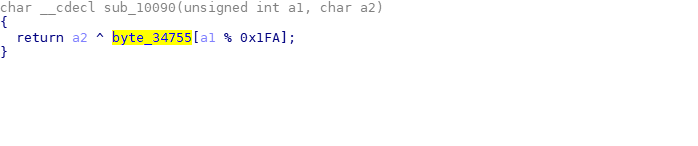
dex\_header()--->dexc\_create()---->sub\_FBF0()



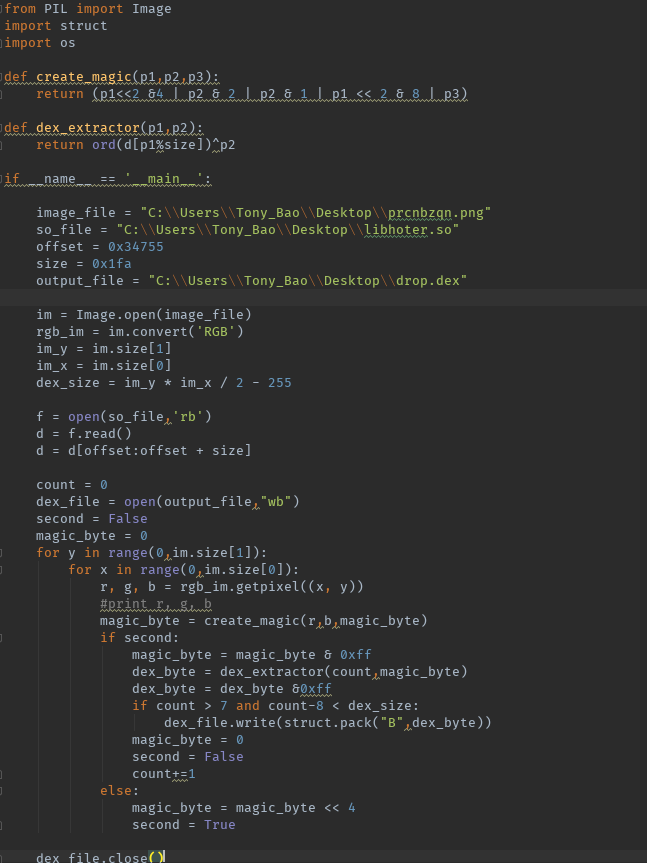
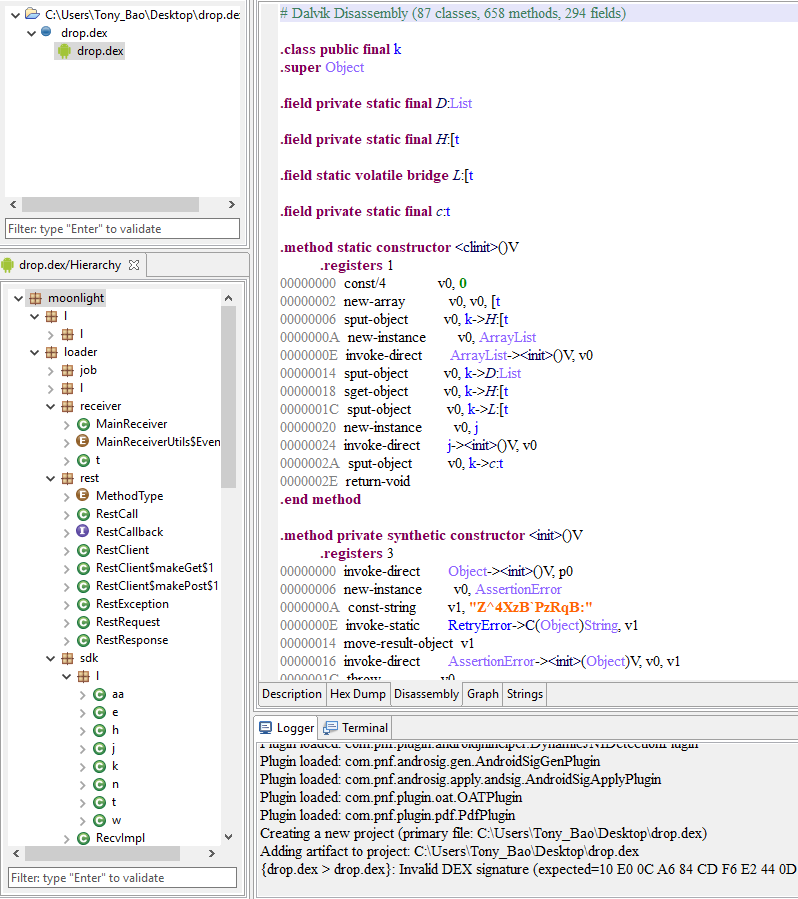
byte\_chooser



Dex extractor



Get dex from png file

Frida script:

