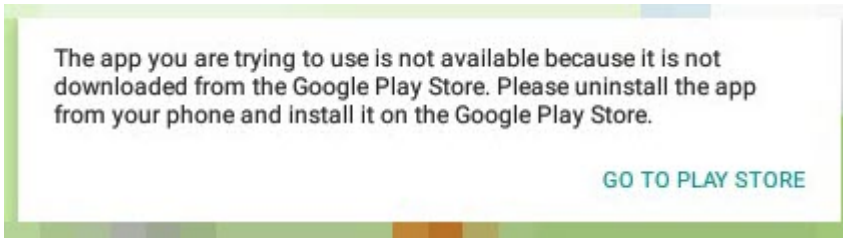
Android’de Kanca Atmak

written by Mert SARICA | 1 January 2021
If you are looking for an English version of this article, please visit here.

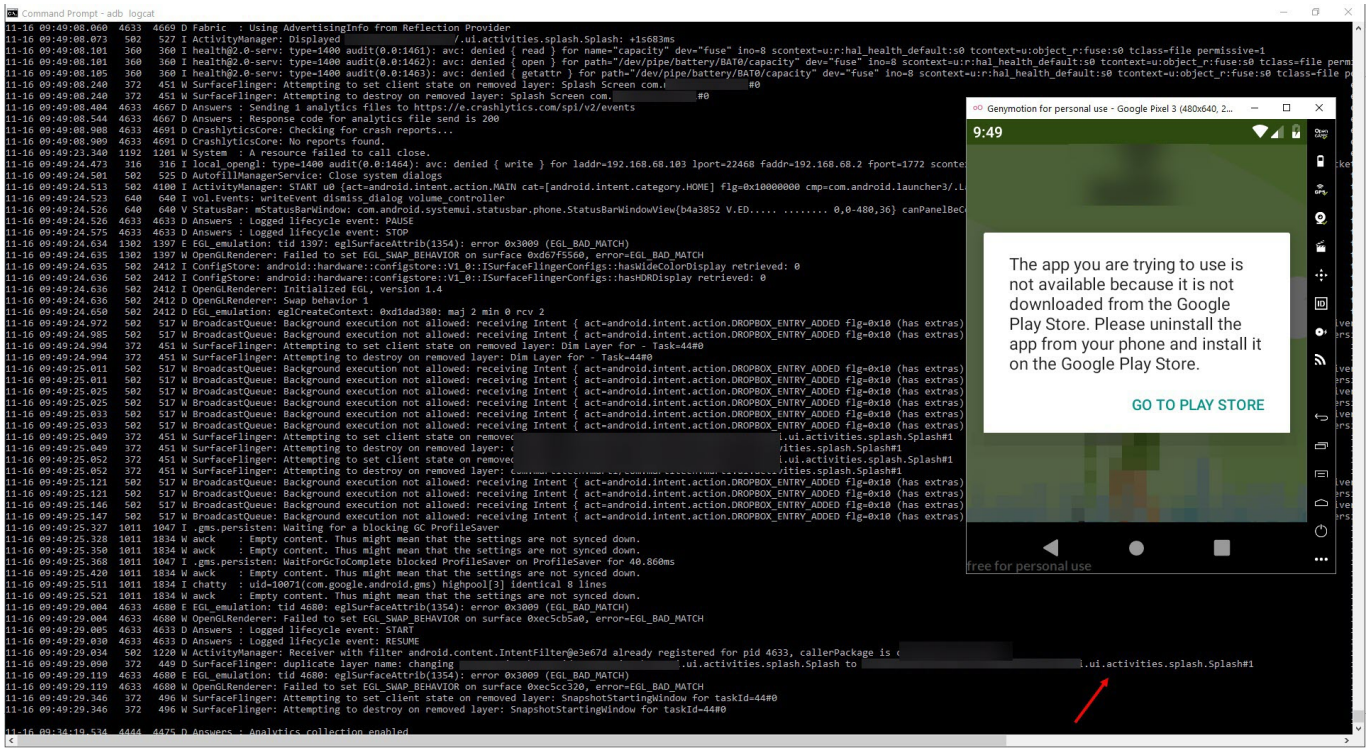
Konumuz Android dünyası olsa da kanca atma denilince nedense aklıma ilk olarak enerji nakil hattına kanca atılarak hanelere çekilen kaçak elektrik gelir. Android dünyasında da aslında uygulamaları dinamik olarak analiz etmek veya müdahale etmek istediğimizde de benzer bir yöntem izleriz. Peki buna neden ihtiyaç duyarız ? Kimi zaman Android uygulamaları ile ilgili bir güvenlik araştırması yapmak istediğimizde veya sızma testi esnasında güvenlik zafiyeti bulmak için hedef Android uygulamasını analiz etme ihtiyacı duyarız. Bunun için genellikle ilk olarak hedef Android uygulamasını kaynak koduna çevirip statik kod analizi yapmakla işe başlarız. Fakat günümüzde çoğu Android uygulamasında kodlar gizlenerek (obfuscation) anlaşılması güçleştirildiği için uygulamayı Genymotion gibi öykünücüler (emulator) üzerinde dinamik olarak analiz etmeye çalışırız. Çalışırız dememin bir sebebi ise yine günümüzde Snapchat gibi mobil uygulamaların statik analizin yanı sıra dinamik analizi de engelleme adına çok sayıda yönteme başvurduğu görülebilmektedir.

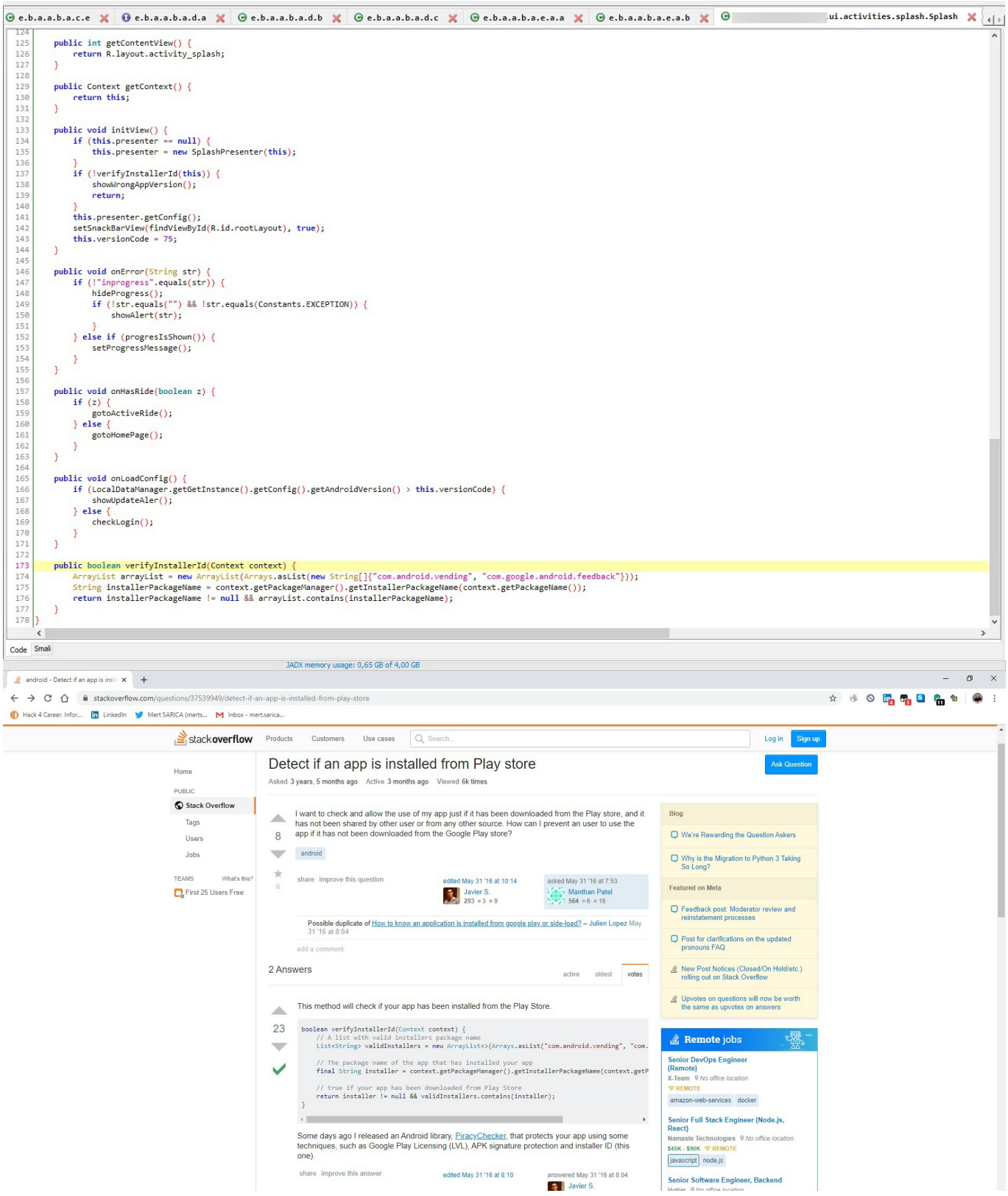
2019 yılının Aralık ayında gerçekleştirdiğim Stockholm seyahatim esnasında şehri gezerken etrafımdan şık şıkırdım insanların vızır vızır elektrikli scooterlar ile geçip gittiğini gördüm. Avrupa’da kullanımının son derece yaygın olması sebebiyle elektrikli scooter uygulamalarının zaman içinde güvenlik araştırmacılarının radarına girmesi ile bazılarında güvenlik zafiyetlerinin tespit edildiğini hatırladım. Ülkemizde de yaygınlaşmaya başlayan elektrikli scooterları ve uygulamalarını kullanmaya başlamadan önce Android uygulamalarından bir tanesinin haberleşmesini, merakımı gidermek amacıyla güvenlik araştırmacısı gözüyle incelemeye karar verdim. Tabii ki her zaman olduğu gibi evdeki hesap çarşıya uymadı ve karşıma çıkan engeller sayesinde ortaya bu blog yazısı çıkmış oldu. :)

Zamanı kısıtlı bir güvenlik araştırmacısı olarak statik kod analizi ile vakit kaybetmek istemediğim için APK dosyasını APK Downloader web uygulaması ile indirip Geny Motion öykünücüsüne yükledim. Uygulamayı çalıştırdıktan sonra karşıma APK dosyasının Google Play üzerinden indirilmemesi sebebiyle sürpriz bir uyarı mesajı çıktı. :)



Bunun üzerine gözü kapalı statik kaynak kodu analizine girmeden önce komut satırında sistem mesajlarını görüntülemek için adb logcat komutunu çalıştırıp ardından da uygulamayı tekrar çalıştırdım. Mesajlar arasından ekrana gelen uyarı mesajı ile ilişkili olduğunu düşündüğüm fonksiyonu bulmak için jadx aracı ile APK dosyasını kaynak koduna çevirdikten sonra activities.splash.Splash dosyasını incelemeye başladım. Dosyanın sonunda yer alan verifyInstallerId fonksiyonu hemen dikkatimi çekti. Bu fonksiyon adını Google arama motorunda arattığımda benzer bir fonksiyonun tam da bu amaçla kullanıldığını gördüm. Bu fonksiyon ile Android'in getInstallerPackageName fonksiyonundan faydalanarak uygulamayı Android'e yükleyen uygulamanın Google Play olup olmadığı kontrol ediliyordu. Şayet uygulama Google Play tarafından işletim sistemine yüklendiyse installerPackagename değişkeni sıfırdan farklı bir değer oluyordu.

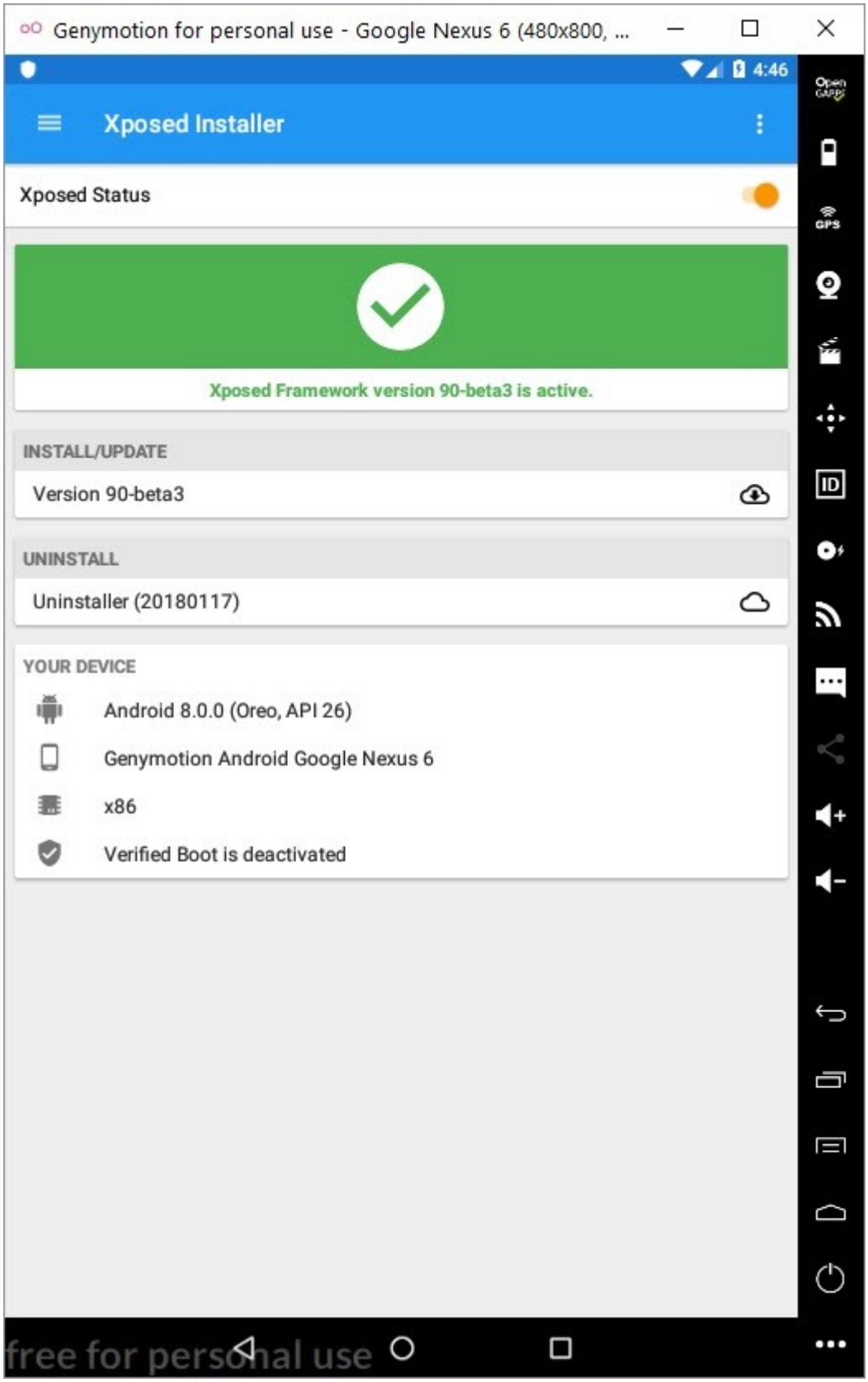


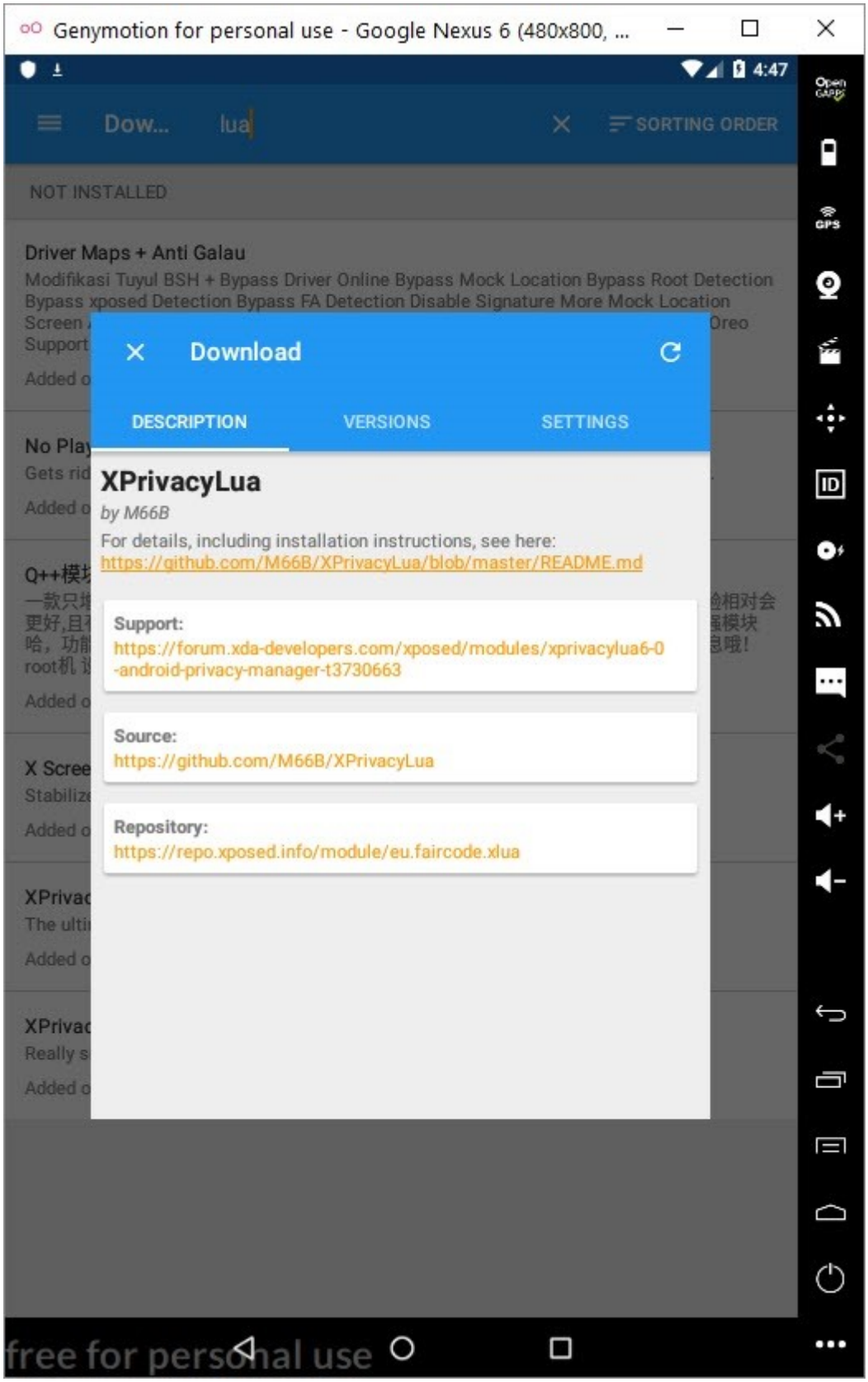


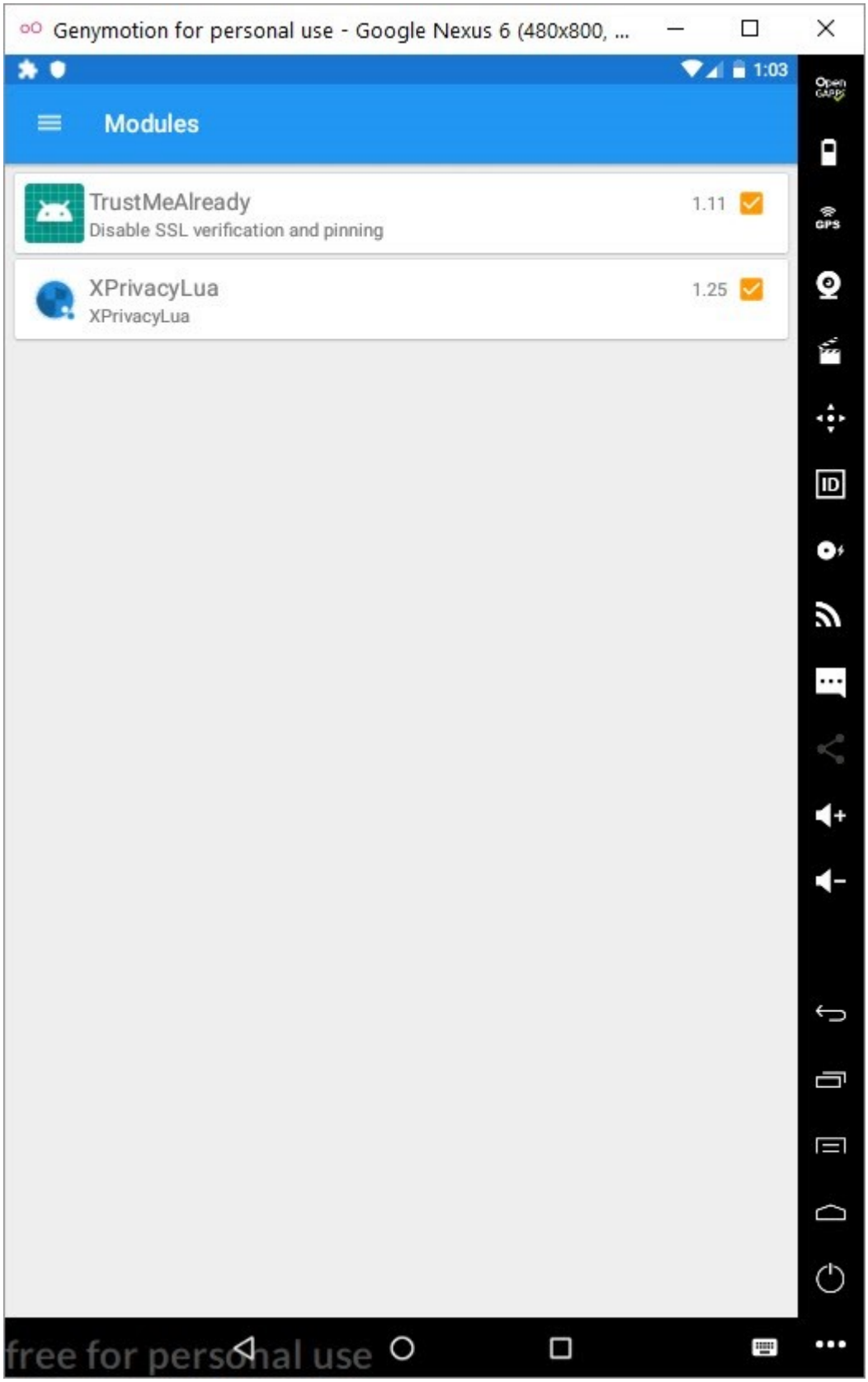
Bu fonksiyona kaynak kodu seviyesinde müdahale edip, installerPackagename değişkenini sıfırdan farklı bir değer yapıp ardından derleyip Android işletim sistemi üzerinde çalıştırabilirdim fakat Bill Gates'in bir röportajında dediği gibi "Her zaman en tembel insanları işe alırım çünkü tembeller çok karışık işleri bile en kısa yoldan yaparlar" ben de tembellik yapıp kısa bir yol aramaya karar verdim. :)

Eminim bu gibi bir durumla karşılaşan güvenlik araştırmacılarının çoğu Frida araç kiti ile ilerlemeyi tercih ederler fakat hayatın Frida'dan ibaret olmaması gerektiğine inanarak Frida'ya alternatif bir araç, farklı bir yol aramaya karar verdim. Google arama motorunda kısa bir araştırma yaptıktan sonra daha önce sızma testlerinde özellikle SSL Pinning'i atlatmak için kullandığım ve 1400'den fazla eklentiye sahip olan Xposed Framework aklıma geldi.

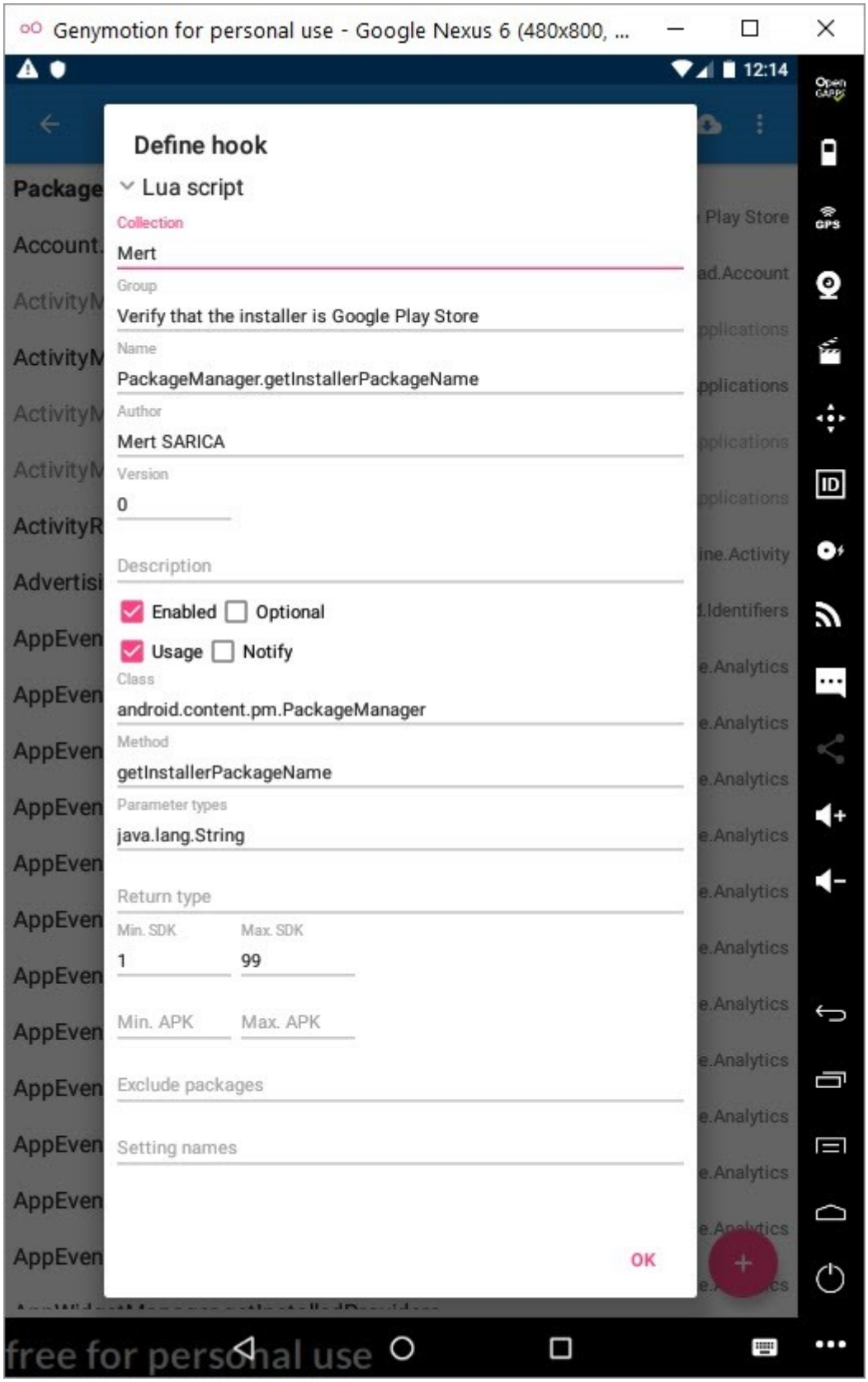
Geny Motion üzerinde bulunan Android Oreo işletim sistemine Xposed Framework'u kurduktan sonra eklentilerine göz atmaya başladım. Eklentiler arasında XPrivaclyLua isimli eklenti hemen dikkatimi çekti. Adından da anlaşılabileceği üzere bu eklenti, Android üzerinde yüklü olan uygulamaları sahte bilgilerle (sahte konum bilgisi gibi) besleyerek mahremiyetinizi korumaya yardımcı olmaktadır. Çalışma yöntemi olarak kabaca bu bilgileri toplamaya çalışan fonksiyonlara kanca atarak gerçek bilgiler yerine sahte bilgiler vermektedir. Eklentiyi ihtiyaçlarınız doğrultusunda şekillendirmek için ise Pro sürümünü yükleyerek Lua programlama dili ile betikler oluşturmanız gerekmektedir.

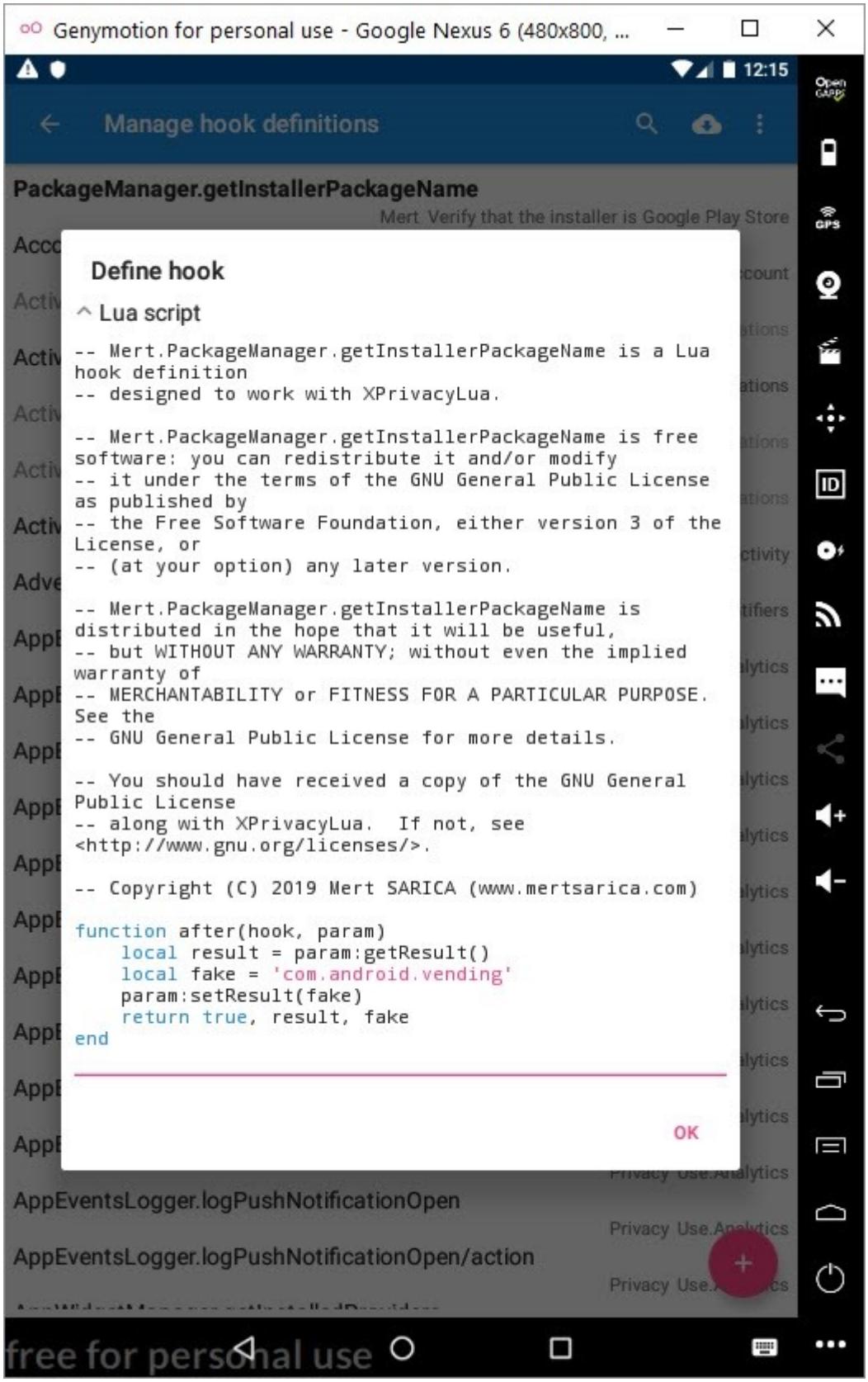

Genymotion for personal use - Google Nexus 6 (480x800, ...
4:46
Xposed Installer
Xposed Status
Xposed Framework version 90-beta3 is active.
INSTALL/UPDATE
Version 90-beta3
UNINSTALL
Uninstaller (20180117)
YOUR DEVICE
Android 8.0.0 (Oreo, API 26)
Genymotion Android Google Nexus 6
x86
Verified Boot is deactivated
free for personal use

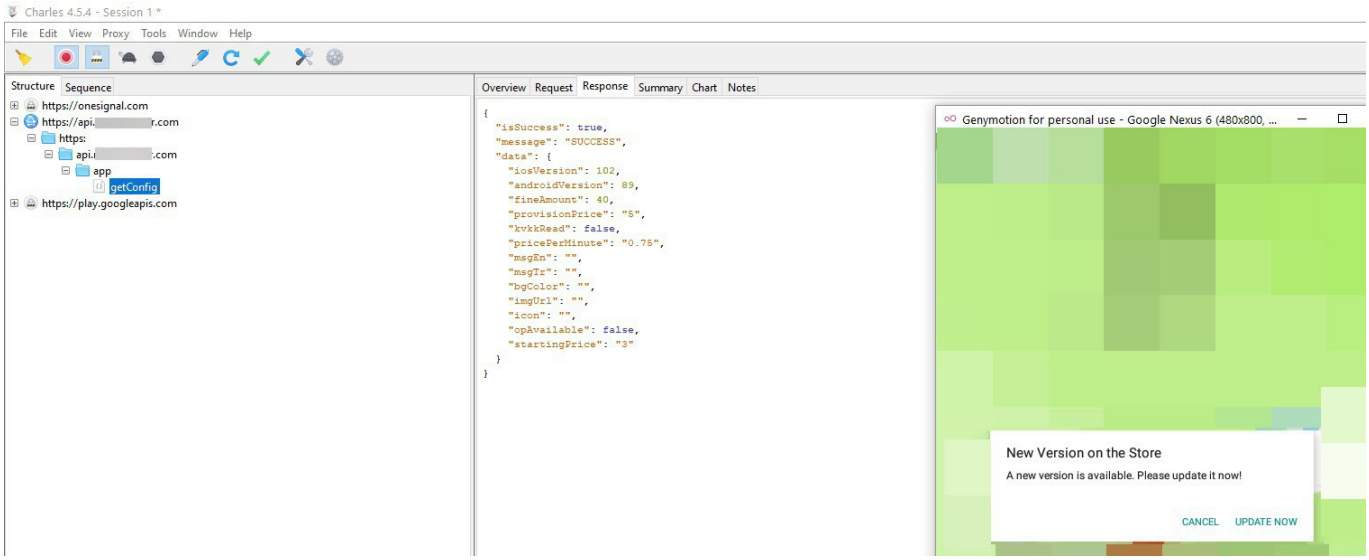

Genymotion for personal use - Google Nexus 6 (480x800, ...
4:47
Dow...
lua
SORTING ORDER
NOT INSTALLED
Driver Maps + Anti Galau
Modifikasi Tuyul BSH + Bypass Driver Online Bypass Mock Location Bypass Root Detection
Bypass xposed Detection Bypass FA Detection Disable Signature More Mock Location
Download
DESCRIPTION
VERSIONS
SETTINGS
XPrivacyLua
by M66B
For details, including installation instructions, see here:
https://github.com/M66B/XPrivacyLua/blob/master/README.md
Support:
https://forum.xda-developers.com/xposed/modules/xprivacylua6-0
-android-privacy-manager-t3730663
Source:
https://github.com/M66B/XPrivacyLua
Repository:
https://repo.xposed.info/module/eu.faircode.xlua
free for personal use



Lua ile installerPackagename değişkenini değiştiren ufak bir betik hazırlayıp aktif hale getirdikten sonra uygulamayı çalıştırdığımda uygulamanın artık daha önceki uyarı mesajını çıkarmadığını ve Charles Proxy ile web trafiğini görüntüleyebildiğimi görerek mutlu sona ulaşmış oldum.


Genymotion for personal use - Google Nexus 6 (480x800, ...
12:14
Define hook
Lua script
Collection
Mert
Group
Verify that the installer is Google Play Store
Name
PackageManager.getInstallerPackageName
Author
Mert SARICA
Version
0
Description
Enabled
Optional
Usage
Notify
Class
android.content.pm.PackageManager
Method
getInstallerPackageName
Parameter types
java.lang.String
Return type
Min. SDK
Max. SDK
1
99
Min. APK
Max. APK
Exclude packages
Setting names
OK
free for personal use


Genymotion for personal use - Google Nexus 6 (480x800, ...
12:15
Manage hook definitions
PackageManager.getInstallerPackageName
Mert Verify that the installer is Google Play Store
Define hook
Lua script
-- Mert.PackageManager.getInstallerPackageName is a Lua hook definition
-- designed to work with XPrivacyLua.
-- Mert.PackageManager.getInstallerPackageName is free software: you can redistribute it and/or modify
-- it under the terms of the GNU General Public License as published by
-- the Free Software Foundation, either version 3 of the License, or
-- (at your option) any later version.
-- Mert.PackageManager.getInstallerPackageName is distributed in the hope that it will be useful,
-- but WITHOUT ANY WARRANTY; without even the implied warranty of
-- MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
-- GNU General Public License for more details.
-- You should have received a copy of the GNU General Public License
-- along with XPrivacyLua. If not, see <http://www.gnu.org/licenses/>.
-- Copyright (C) 2019 Mert SARICA (www.mertsarica.com)
function after(hook, param)
local result = param:getResult()
local fake = 'com.android.vending'
param:setResult(fake)
return true, result, fake
end
OK
AppEventsLogger.logPushNotificationOpen
AppEventsLogger.logPushNotificationOpen/action
free for personal use



Bu yazının güvenlik araştırmalarında Frida'ya alternatif araç ve yöntem arayanlara ışık tutacağını ümit ederek bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.