

Google Play Protect - Detection Bypass

دور زدن سپر ایمنی گوگل پلی

**نویسنده : آرین چهرقانی**

**چکیده :**

در این سند به معرفی سپر ایمنی گوگل پلی ، مراحلی که برای دورزدن ( تشخیص ورودی های ناامن ) در سپر محافظتی گوگل پلی به کار گرفته شده میپردازیم ،

آزمایش های زیادی روی سپر ایمنی گوگل پلی صورت گرفته است ( تغییر امضا – افزیش و کاهش حجم بسته نصبی - بایند کردن بسته نصبی – دریافت خروجی جدید از بسته مخرب و . . . )

اما ، ما قصد داریم که در این سند به دورزدن مکانیزم شناسایی برنامه های مخرب توسط سپر ایمنی گوگل پلی با یک روش فوق العاده ساده بپردازیم !

فهرست

چکیده1

مقدمه2

نصب ویرایشگر3

مراحل4

توضیحات5

پایان6

**[سپر ایمنی گوگل پلی – مقدمه]**

**این سرویس هنگامی که برنامه‌ای را نصب می‌کنید آن را بررسی می‌کند تا از صحت آن اطمینان حاصل کند و مطمئن شود که این اپلیکیشن مخرب نیست یا دسترسی‌های خطرناک ندارد. همچنین به صورت دوره‌ای گوشی شما را بررسی می‌کند تا از موبایل شما در برابر برنامه‌های مخرب محافظت کند .**

**این برنامه هنگامی که برنامه‌ای مضر در گوشی شما پیدا کند، بسته به میزان خطر به دو روش عمل می‌کند .**

**روش اول هنگامی استفاده می‌شود که برنامه مضر پیدا شده، آنقدرها هم خطرناک نیست. در این روش برنامه مضر متوقف می‌شود و شما اعلانی مبنی بر مضر بودن و توصیه به حذف آن دریافت می‌کنید.**

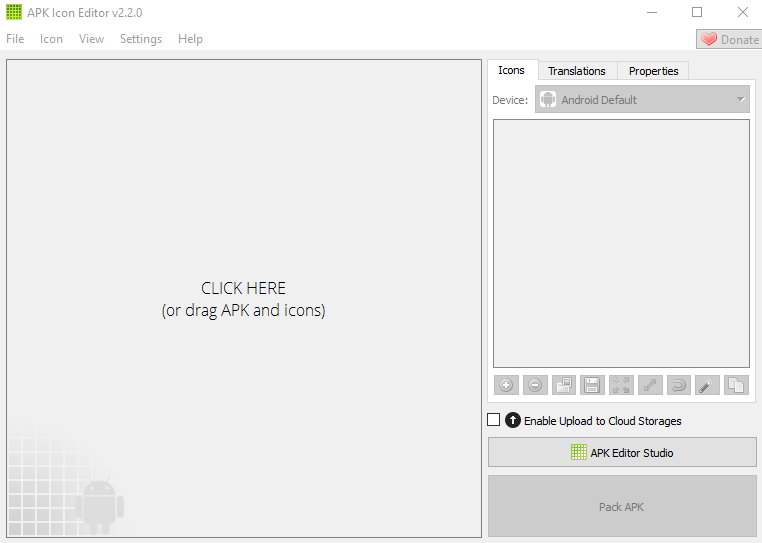
**روش دوم مخصوص زمانی است که برنامه خطرناک پیدا شده، شدیداً امنیت گوشی و اطلاعات شما را تهدید می‌کند. در این زمان است که play protect یا سپر ایمنی گوگل دست به کار می‌شود و بدون اطلاع دادن به شما، برنامه را حذف می‌کند .**

*نمونه این موقعیت، حذف دو پوسته محبوب تلگرام یعنی “تلگرام طلایی” و “هاتگرام” از روی گوشی‌ها بود .*

**سپر ایمنی گوگل همواره از طریق یادگیری ماشینی در حال بهبود است و در آینده می‌توان منتظر بهتر شدن و پیشرفت چشمگیر این قابلیت بود. به امید دنیایی بدون برنامه‌های مخرب .**

[نصب ویرایشگر]

APK Icon Editor - v2.2.0

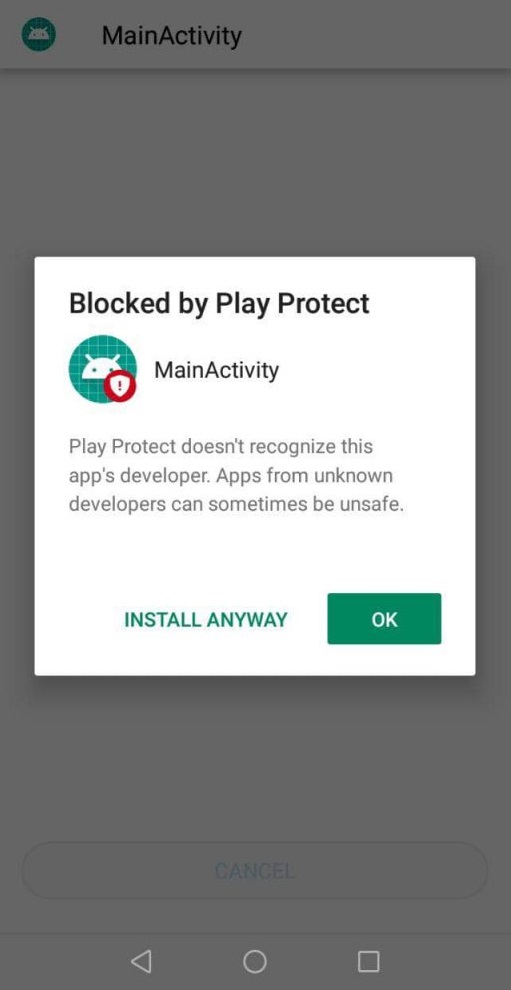


Download :

<https://softsara.ir/apk-icon-editor>

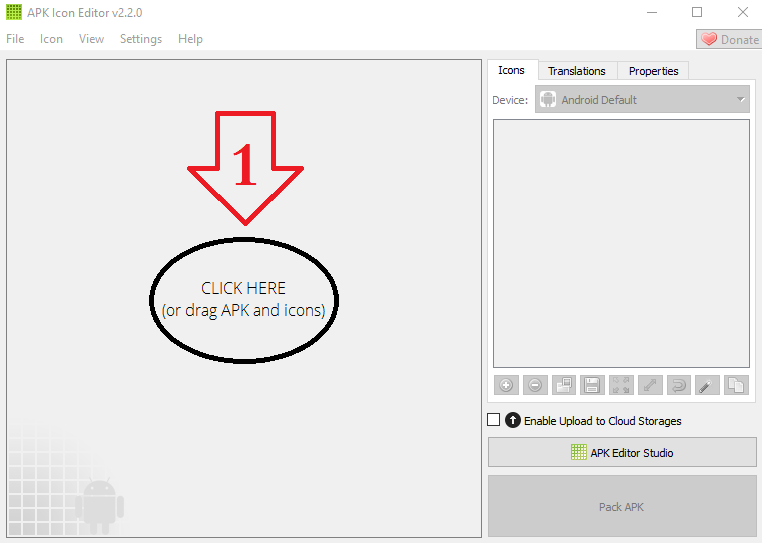
[مراحل]

1 - یک بسته مخرب را نصب میکنیم :



\*مشاهده میکنیم که بسته با موفقیت نصب نشد و شناسایی شد

2 – وارد ویرایشگر میشویم و بسته مخرب را وارد میکنیم :



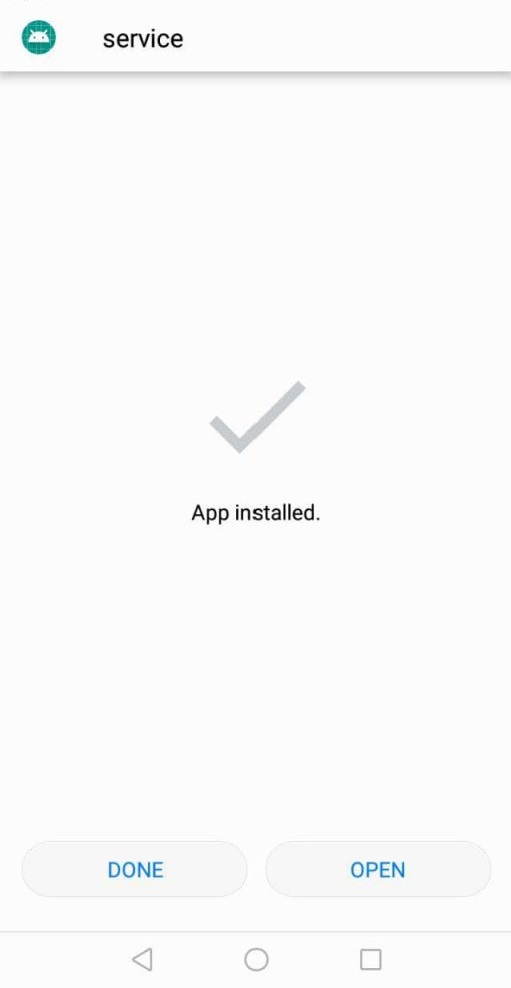
4 – سپس در قسمت :

" Properties" =🡺 "TARGET SDK"

5 - مقدار پیش فرض را به عددی خارج از خط قرمز تغییر میدهیم :

برای مثال : "39"

6 – مجدد بسته مخرب را نصب میکنیم و **مشاهده میکنیم بسته مخرب با موفقیت کامل نصب شد**



[توضیحات]

هر نسخه جدید اندروید تغییراتی را ایجاد می کند که باعث بهبود قابل توجه امنیت و عملکرد و همچنین افزایش تجربه کاربری اندروید به طور کلی می شود. برخی از این تغییرات فقط در مورد برنامه هایی اعمال می شود که صراحتاً از طریق مشخصه

targetSdkVersion

پشتیبانی خود را اعلام می کنند.

<https://developer.android.com/distribute/best-practices/develop/target-sdk>

[پایان]

امیدوارم که لذت برده باشید سعی کردیم خیلی خلاصه مطلب رو منتقل کنیم و انتظار داریم راحت به هر انتی ویروسی اعتماد نکنید حتی اگر اون انتی ویروس از بهترین شرکت های جهان باشه و سابقه خوبی داشته باشه در این مورد !   
  
با سپاس فراوان از شما دوستان عزیز و همراهان همیشگی

باتشکر از دوست عزیزم :

* Sajjadbnd | Biskooit Pedar