看雪3万课程笔记-FRIDA高级API实用方法：Frida Hook Java（八）APP启动时进行hook

原创

kfyzjd2008 于 2022-02-18 14:33:37 发布 232 收藏
分类专栏： 安卓 文章标签： frida hook 安卓逆向 frida 看雪三万 安卓hook

本文链接：https://blog.csdn.net/kfyzjd2008/article/details/123002339

此节可开始使用APP为：kgb-messenger.apk

本节知识点：

APP启动时进行HOOK，命令如下：

```
frida -U --no-pause -f com.tlamb96.spetsnazmessenger -l hook.js
//关键命令    --no-pause -f
```

java使用的系统命令库地址为：

java.lang.* 例如：Java.use("java.lang.System");

java中R为前缀的资源内容可以在以下路径中查找，例如字符资源：

jadx中 资源文件 -> resources.arsc -> res -> values -> strings.xml

正文：

```
public void onCreate(Bundle bundle) {
    super.onCreate(bundle);
    setContentView(R.layout.activity_main);
    String property = System.getProperty("user.home");
    String str = System.getenv("USER");
    if (property == null || property.isEmpty() || !property.equals("Russia")) {
        a("Integrity Error", "This app can only run on Russian devices.");
    } else if (str == null || str.isEmpty() || !str.equals(getResources().getString(R.string.User))) {
        a("Integrity Error", "Must be on the user whitelist.");
    } else {
        a.a(this);
        startActivity(new Intent(this, LoginActivity.class));
    }
}
```

两处判断点

判断点一直接让函数返回“Russia”即可

判断点二在资源中找到User的值然后返回。

具体代码如下：

```
function hook_java(){
    Java.perform(function(){
        var System = Java.use("java.lang.System");
        console.log(System);
        System.getProperty.overload('java.lang.String').implementation = function(key){
            var result = this.getProperty(key);
            result = "Russia";
            console.log("System.getProperty:",key,result);
            return result;
        };

        System.getenv.overload('java.lang.String').implementation = function(key){
            var result = this.getenv(key);
            result = "RkxBR3s1N0VSTDFOR180UkNIM1J9Cg=="
            console.log("System.getenv:",key,result);
            return result;
        };

    })
}
```