|  |  |  |
| --- | --- | --- |
| 资源 | 途径 | 效果 |
| 界面数据 | 1、通过重写Application中回调函数获取Activity实例 | 窃取用户输入的明文密码 |
| 2、通过ActivityThread类中静态成员sActivityThread获取Activity实例 |
| 3、获取Activity的一些Textview等字段，可以更改其界面UI | 更改UI界面 |
| Http连接池 | 1、访问ConfigAwareConnectionPool中的instance字段，获取并关闭连接池 | 清空连接池 |
| 2、访问ConnectPool中的connections字段，获取其连接信息 | 获取连接信息 |
| 手机App信息 | 利用PackageManager可以得到本机上所有已安装App的信息，包括应用权限包名，类名等 | 窃取手机App信息 |
| Activity  Service等 | 1、调用getDefault方法获取ActivityManagerNative中唯一的远程服务接口，进行启动Activity等 | 启动Activity |
| 2、访问ActivityManagerNative中的gDefault字段，将其保存的远程服务接口实例替换为自己的代理接口。 | 替换远程服务接口 |
| 线程Looper | 调用getMainLooper得到线程Looper，修改MessageQueue中mquitAllowed字段，之后quit | 强制退出进程 |
| 宿主的类 | DexPathList类中的dexElements字段记录了宿主程序的dex列表，可以加载外部代码并插入到dex列表中 | 替换宿主的类 |
|  |  |  |

SDK攻击途径总结