MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

汇创ERP 1.2.APK

APP名称:	汇创ERP
包名:	com.hcwot.hcerp
域名线索:	5条
URL线索:	5条
邮箱线索:	0条
分析日期:	2022年2月2日 20:08

文件信息

文件名: hcerp.apk
文件大小: 2.46MB
MD5值: 1797bcb4960741219ecef8223c608bef
SHA1值: 01c38124b8b0069e5e5d209feaaca069482e1bdd
SHA256值: 5fbcabf53a5cfe95d175cdb32d1b55f5ca1303d516f742b4ca3f4f91734f3f96

APP 信息

App名称: 汇创ERP
包名: com.hcwot.hcerp
主活动**Activity:** com.djj.webviewdemo.MainActivity
安卓版本名称: 1.2
安卓版本: 24

域名线索

域名	是否危险域名	服务器信息
android.bugly.qq.com	good	**IP:** 109.244.244.35 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map

域名	是否危险域名	服务器信息
astat.bugly.qcloud.com	good	**IP:** 150.109.29.135 **所属国家:** Korea (Republic of) **地区:** Seoul-teukbyeolsi **城市:** Seoul **纬度:** 37.568260 **经度:** 126.977829 **查看地图:** Google Map
rqd.uu.qq.com	good	**IP:** 182.254.88.185 **所属国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看地图:** Google Map
aexception.bugly.qq.com	good	**IP:** 101.226.233.161 **所属国家:** China **地区:** Shanghai **城市:** Shanghai **纬度:** 31.222219 **经度:** 121.458061 **查看地图:** Google Map
erp.hcwot.com	good	**IP:** 39.97.123.222 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
http://erp.hcwot.com/	com/djj/webviewdemo/MainActivity.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/beta/upgrade/BetaUploadStrategy.java
http://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/crashreport/CrashReport.java
http://rqd.uu.qq.com/rqd/sync	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
http://aexception.bugly.qq.com:8012/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java

此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像

向手机申请的权限	是否危险	类型	详细情况
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
android.permission.ACCESS_WIFI_STATE	正常	查看Wi-Fi状态	允许应用程序查看有关 Wi-Fi 状态的信息
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=CHN, ST=liaoning, L=shenyang, O=huichuang, OU=huichuang, CN=huichuang
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-06-26 03:00:01+00:00
Valid To: 2045-06-20 03:00:01+00:00
Issuer: C=CHN, ST=liaoning, L=shenyang, O=huichuang, OU=huichuang, CN=huichuang
Serial Number: 0x5cf4e2f

Hash Algorithm: sha256
md5: 68298f1ec6e4c36c60f2242486fb651b
sha1: 74a1d53b6f898fc2b3721802fbee1b05aa72d73c
sha256: 7aca969838bdf20663b3a3c86c9e1baa5e6dbe61015bd5f557ebfd2ea6baacac
sha512: 288f1ed005a708f0d67446c79a0159757df96da9c837cf0d5e8063c7532a3d1bd282f85468d8dd241ecdf7c38006a0867d88c6b0338622313dfd8f756a034c8f
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 34f2a061708a15b5dc7de900df37853a06c18501f2cf12186a742cc27f1af835

Exodus威胁情报

名称	分类	URL链接
Bugly		https://reports.exodus-privacy.eu.org/trackers/190

加壳分析

文件列表	分析结果

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>Build.MODEL check
Build.PRODUCT check
possible Build.SERIAL check
Build.TAGS check
possible ro.secure check
emulator file check</td></tr>
<tr><td>编译器</td><td>dx (possible dexmerge)</td></tr>
<tr><td>Manipulator Found</td><td>dexmerge</td></tr>
</table>
</td></tr>
</table>
