MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

Unily 6.3.0.APK

APP名称:	Unily
包名:	com.unily.china
域名线索:	23条
URL线索:	33条
邮箱线索:	0条
分析日期:	2022年2月2日 23:04

文件信息

文件名: Unily562488.apk
文件大小: 8.24MB
MD5值: 1f71f32eedb8be9dc84633302bc1811c
SHA1值: 4f7f3e7489ac513fec115c1d34fd5304187fd4c4
SHA256值: 341ee6477c23339db3f907f9937a9cac44c169b299ed45210e71b235dccc1ef5

APP 信息

App名称: Unily
包名: com.unily.china
主活动Activity: com.brightstarr.unily.StartupActivity
安卓版本名称: 6.3.0
安卓版本: 8

域名线索

域名	是否危险域名	服务器信息
login.chinacloudapi.cn	good	**IP:** 52.130.17.193 **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
login.microsoftonline.us	good	**IP:** 52.126.194.129 **所属国家:** United States of America **地区:** Iowa **城市:** Des Moines **纬度:** 41.600540 **经度:** -93.609108 **查看地图:** Google Map
msmamservice.api.application	good	没有服务器地理信息.
10.95.41.15	good	**IP:** 10.95.41.15 **所属国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看地图:** Google Map

域名	是否危险域名	服务器信息
login.microsoftonline.com	good	**IP:** 40.126.16.165 **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
mobile.events.data.microsoft.com	good	**IP:** 104.208.16.89 **所属国家:** United States of America **地区:** Iowa **城市:** Des Moines **纬度:** 41.600540 **经度:** -93.609108 **查看地图:** Google Map
appconfig.unily.com	good	**IP:** 52.166.181.39 **所属国家:** Netherlands **地区:** Noord-Holland **城市:** Amsterdam **纬度:** 52.374031 **经度:** 4.889690 **查看地图:** Google Map
intunemam.microsoftonline.com	good	没有服务器地理信息.
login.microsoftonline.de	good	**IP:** 51.4.145.158 **所属国家:** Germany **地区:** Hessen **城市:** Frankfurt am Main **纬度:** 50.115520 **经度:** 8.684170 **查看地图:** Google Map

域名	是否危险域名	服务器信息
login.partner.microsoftonline.cn	good	**IP:** 52.130.17.192 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
login.windows.net	good	**IP:** 20.190.163.20 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067 查看地图: Google Map
github.com	good	**IP:** 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903 查看地图: Google Map
schemas.android.com	good	没有服务器地理信息.
in.appcenter.ms	good	**IP:** 40.70.161.102 所属国家: United States of America 地区: Virginia 城市: Boydton 纬度: 36.667641 经度: -78.387497 查看地图: Google Map

域名	是否危险域名	服务器信息
180.76.76.112	good	**IP:** 180.76.76.112 **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
login.windows-ppe.net	good	**IP:** 20.190.144.167 **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
www.slf4j.org	good	**IP:** 83.173.251.158 **所属国家:** Switzerland **地区:** Zurich **城市:** Zurich **纬度:** 47.366669 **经度:** 8.550000 **查看地图:** Google Map
appassets.androidplatform.net	good	没有服务器地理信息.
api.tuisong.baidu.com	good	**IP:** 110.242.69.51 **所属国家:** China **地区:** Hebei **城市:** Baoding **纬度:** 38.851109 **经度:** 115.490280 **查看地图:** Google Map

域名	是否危险域名	服务器信息
devicemgmt.teams.microsoft.com	good	**IP:** 52.114.159.152 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.774929 经度: -122.419418 查看地图: Google Map
www.example.com	good	**IP:** 93.184.216.34 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.043720 经度: -77.487488 查看地图: Google Map
go.microsoft.com	good	**IP:** 23.212.234.61 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: London 纬度: 51.508530 经度: -0.125740 查看地图: Google Map
clients3.google.com	good	**IP:** 142.251.42.238 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514 查看地图: Google Map

URL线索

URL信息	Url所在文件
https://go.microsoft.com/fwlink/?linkid=534633	com/microsoft/intune/mam/client/app/AppStoreUtils.java
https://login.windows.net/common/	com/microsoft/intune/mam/client/app/startup/ADALConnectionDetails.java
https://intunemam.microsoftonline.com	com/microsoft/intune/mam/client/app/startup/ADALConnectionDetails.java
https://login.windows.net	com/microsoft/intune/mam/http/KnownClouds.java
https://go.microsoft.com/fwlink/?LinkID=533051&clcid=0x409	com/microsoft/intune/mam/http/KnownClouds.java
https://login.microsoftonline.us	com/microsoft/intune/mam/http/KnownClouds.java
https://go.microsoft.com/fwlink/?linkid=851103	com/microsoft/intune/mam/http/KnownClouds.java
https://login.chinacloudapi.cn	com/microsoft/intune/mam/http/KnownClouds.java
https://login.microsoftonline.de	com/microsoft/intune/mam/http/KnownClouds.java
https://msmamservice.api.application	com/microsoft/intune/mam/policy/MAMServiceAuthentication.java
http://schemas.android.com/apk/res/android	com/microsoft/intune/mam/policy/appconfig/AndroidEnterpriseAppConfigUtil.java
https://login.partner.microsoftonline.cn	com/microsoft/identity/client/AzureCloudInstance.java
https://login.microsoftonline.de	com/microsoft/identity/client/AzureCloudInstance.java
https://login.microsoftonline.us	com/microsoft/identity/client/AzureCloudInstance.java
https://go.microsoft.com/fwlink/?linkid=2138180	com/microsoft/identity/common/internal/ui/webview/OAuth2WebViewClient.java
http://www.example.com	com/microsoft/identity/common/internal/ui/browser/BrowserSelector.java
https://devicemgmt.teams.microsoft.com/.default	com/microsoft/identity/common/internal/migration/TokenCacheItemMigrationAdapter.java
https://login.windows-ppe.net	com/microsoft/identity/common/internal/providers/microsoft/azureactivedirectory/AzureActiveDirectoryEnvironment.java

URL信息	Url所在文件
https://login.microsoftonline.com	com/microsoft/identity/common/internal/providers/microsoft/azureactivedirectory/AzureActiveDirectoryEnvironment.java
https://login.microsoftonline.com/microsoft.com/oauth2/token	com/microsoft/identity/common/internal/providers/microsoft/azureactivedirectory/AzureActiveDirectoryOAuth2Strategy.java
https://login.microsoftonline.com/common/oauth2/v2.0/authorize	com/microsoft/identity/common/internal/providers/microsoft/azureactivedirectory/AzureActiveDirectory.java
https://login.microsoftonline.com/common/oauth2/v2.0/logout	com/microsoft/identity/common/adal/internal/AuthenticationConstants.java
https://go.microsoft.com/fwlink/?linkid=2138180	com/microsoft/identity/common/adal/internal/AuthenticationConstants.java
https://login.microsoftonline.com/consumers	com/microsoft/identity/common/adal/internal/tokensharing/TokenShareUtility.java
https://login.windows.net/common	com/microsoft/identity/common/adal/internal/tokensharing/TokenShareUtility.java
http://10.95.41.15:8080	com/baidu/android/pushservice/h.java
https://api.tuisong.baidu.com/rest/3.0/clientfile/updateconfig	com/baidu/android/pushservice/b/d.java
https://180.76.76.112/v6/0025?type=ipv4,ipv6&dn=	com/baidu/android/pushservice/d/j.java
https://appconfig.unily.com/	com/brightstarr/unily/h1.java
https://appassets.androidplatform.net/assets/	com/brightstarr/unily/LocalContentWebViewActivity.java
http://www.slf4j.org/codes.html#no_static_mdc_binder	org/slf4j/MDC.java
http://www.slf4j.org/codes.html#null_MDCA	org/slf4j/MDC.java
http://www.slf4j.org/codes.html	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#multiple_bindings	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#StaticLoggerBinder	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#null_LF	org/slf4j/LoggerFactory.java

URL信息	Url所在文件
http://www.slf4j.org/codes.html#substituteLogger	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#unsuccessfulInit	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#version_mismatch	org/slf4j/LoggerFactory.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	e/a/b.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	e/a/k.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	e/a/f.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	e/a/h.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	e/a/r.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	e/a/y/f.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	e/a/y/d.java
http://clients3.google.com/generate_204	d/a/a/a/a/a/c/a/a.java
https://mobile.events.data.microsoft.com/OneCollector/1.0	d/d/a/m/c.java
https://in.appcenter.ms	d/d/a/m/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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字

向手机申请的权限	是否危险	类型	详细情况
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.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
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.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
android.permission.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加和删除帐户以及删除其密码等操作
android.permission.USE_CREDENTIALS	危险	使用帐户的身份验证凭据	允许应用程序请求身份验证令牌
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_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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
baidu.push.permission.WRITE_PUSHINFOPROVIDER.com.unily.china	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取

向手机申请的权限	是否危险	类型	详细情况
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=Tim Moxon, OU=Development, O=Bright Starr Ltd, L=Godalming, C=GB
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-03-10 15:32:16+00:00
Valid To: 2066-02-26 15:32:16+00:00
Issuer: CN=Tim Moxon, OU=Development, O=Bright Starr Ltd, L=Godalming, C=GB
Serial Number: 0x1ee9bca7
Hash Algorithm: sha256
md5: 83352537ea669d8dfad1c4ac5ab2539b
sha1: 6d54c14a51448c22356c1ab27cce53ace5a6733d
sha256: d7668b0ad23c270622183a1383833d2dfaef626f165e112033a0e75fb13990fd
sha512: cdfe85212d1d57a6470f6a4ed780186cbdf6ea1625b1e31caa367c942bfa2a82336b659ad44f66005731b8529bc2081a11a2cc2564822070bb45d22a52c45269
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 4687ee28a52d21d613d8fbe0e458be990bdda9186f31a8d74158cfa3ed712fcc

Exodus威胁情报

名称	分类	URL链接
Microsoft Visual Studio App Center Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/243
Microsoft Visual Studio App Center Crashes	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/238

硬编码敏感信息

可能的敏感信息
"firebase_preference_file_key" : "com.microsoft.windowsazure.messaging.notificationhubs.FirebasePreferences"
"http_auth_dialog_cancel" : "Cancel"
"http_auth_dialog_login" : "Login"
"http_auth_dialog_password" : "Password"
"http_auth_dialog_title" : "Enter your credentials"
"http_auth_dialog_username" : "Username"
"installation_enrichment_file_key" : "com.microsoft.windowsazure.messaging.notificationhubs.InstallationSharedPreferences"

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.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible Build.SERIAL check
SIM operator check
network operator name check</td></tr>
<tr><td>反调试</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>