MoGua

CreeperBox 1.0.APK 分析报告

APP名称:	CreeperBox
包名:	helper.creeperbox
域名线索:	7条
URL线索:	12条
邮箱线索:	5条
分析日期:	2025年7月2日

分析平台: 摸瓜APK反编译平台

文件信息

文件名: CreeperBox1.0.6.apk
文件大小: 37.54MB
MD5值: dc89e798c5a320998446e3e7580826ff
SHA1值: 275c9328e45a91b04824c2a05a4fd8dca8a05668
SHA256值: aa8d141d9d13cb95fe845dcd5c237f001094f2311530a3ecc9f2f410ed130150

APP 信息

App名称: CreeperBox
包名: helper.creeperbox
主活动Activity:
安卓版本名称: 1.0
安卓版本: 1

域名线索

域名	服务器信息
netty.io	**IP**: 172.67.130.186 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
	IP: 40.126.35.150 **所属国家**: Singapore

login.live.com	**地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
www.openssl.org	IP: 34.49.79.89 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
tools.ietf.org	IP: 104.16.44.99 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.slf4j.org	IP: 195.15.222.169 **所属国家**: Switzerland **地区**: Geneve **城市**: Carouge **纬度**: 46.180931 **经度**: 6.138709
www.eclipse.org	IP: 198.41.30.198 **所属国家**: Canada **地区**: Ontario **城市**: Brampton **纬度**: 43.702347 **经度**: -79.711548
wiki.eclipse.org	IP: 198.41.30.195 **所属国家**: Canada **地区**: Ontario **城市**: Brampton **纬度**: 43.702347 **经度**: -79.711548

URL线索

URL**信息**	Url**所在文件**
https://tools.ietf.org/html/rfc7540	io/netty/handler/codec/http2/HttpConversionUtil.java
https://wiki.eclipse.org/Jetty/Feature/NPN	io/netty/handler/ssl/JdkNpnApplicationProtocolNegotiator.java
https://netty.io/wiki/forked-tomcat-native.html	io/netty/handler/ssl/OpenSsl.java
https://www.openssl.org/docs/man1.0.2/apps/verify.html.	io/netty/handler/ssl/OpenSslCertificateException.java
https://netty.io/wiki/sslcontextbuilder-and-private-key.html	io/netty/handler/ssl/PemReader.java

https://www.eclipse.org/jetty/documentation/current/alpn-chapter.html	io/netty/handler/ssl/JdkAlpnApplicationProtocolNegotiator.java
https://netty.io/wiki/reference-counted-objects.html	io/netty/util/ResourceLeakDetector.java
https://login.live.com/oauth20_authorize.srf? client_id=00000000441cc96b&redirect_uri=https://login.live.com/oauth20_desktop.srf&response_type=token&display=touch&scope=service::user.auth.xboxlive.com::MBI_SSL&locale=en	org/cloudburstmc/protocol/bedrock/util/XblUtils.java
https://login.live.com/oauth20.srf	org/cloudburstmc/protocol/bedrock/util/XblUtils.java
https://tools.ietf.org/html/rfc7797	org/jose4j/jws/JsonWebSignature.java
http://www.slf4j.org/codes.html	org/slf4j/MDC.java
http://www.slf4j.org/codes.html	org/slf4j/LoggerFactory.java

邮箱线索

邮箱地址	所在文件
e@m15_hjsi1.b6	helper/creeperbox/gj.java
mjdi@oxf.qnx	摸瓜V2引擎
z@x.dű	摸瓜V2引擎
ﾍ@□ɲ.dq	摸瓜V2引擎
o@as.ize eu@z9.xhk to1j@w.eè929dit 1ą@l.ee	摸瓜V2引擎

手机线索

手机号	所在文件
17179869183	org/msgpack/core/MessageUnpacker.java

签名证书

APK已签名
v1 签名: True
v2 签名: True

v3 签名: True
找到 1 个唯一证书
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
md5值: e89b158e4bcf988ebd09eb83f5378e87
sha1值: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
sha256值: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
sha512值: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569
公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75

硬编码敏感信息

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

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
android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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
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
helper.creeperbox.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信