前言	1.1
绕过抓包限制概述	1.2
绕过证书绑定	1.3
Android	1.3.1
信任证书问题	1.3.1.1
Xposed插件	1.3.1.2
JustTrustMe	1.3.1.2.1
TrustMeAlready	1.3.1.2.2
iOS	1.3.2
插件	1.3.2.1
SSL Kill Switch	1.3.2.1.1
SSLBypass	1.3.2.1.2
其他特殊处理	1.4
<u>抖音</u>	1.4.1
Android版	1.4.1.1
Frida去hook代码	1.4.1.1.1
修改并替换libsscronet.so库文件	1.4.1.1.2
iOS版	1.4.1.2
附录	1.5
参考资料	1.5.1

移动端逆向:绕过抓包限制

- 最新版本: 0.8.0
- 更新时间: 20250603

简介

整理移动端逆向期间,关于如何绕过各种抓包的限制;包括绕过证书绑定和其他一些特殊处理;绕过证书 绑定又包括iOS端和安卓端,比如iOS端的插件,比如SSL Kill Switch的ssl-kill-switch3和SSL Kill Switch 2,以及SSLBypass等插件等去实现绕过ssl证书绑定从而破解https;安卓端的Xposed模块,包括 TrustMeAlready、JustTrustMe等等;其他特殊处理包括抖音的iOS版和Android版的一些特定处理等等;

源码+浏览+下载

本书的各种源码、在线浏览地址、多种格式文件下载如下:

HonKit源码

• crifan/mobile_re_capture_bypass_limit: 移动端逆向: 绕过抓包限制

如何使用此HonKit源码去生成发布为电子书

详见: crifan/honkit_template: demo how to use crifan honkit template and demo

在线浏览

- 移动端逆向:绕过抓包限制 book.crifan.org
- 移动端逆向:绕过抓包限制 crifan.github.io

离线下载阅读

- 移动端逆向:绕过抓包限制 PDF
- 移动端逆向:绕过抓包限制 ePub
- 移动端逆向:绕过抓包限制 Mobi

版权和用途说明

此电子书教程的全部内容,如无特别说明,均为本人原创。其中部分内容参考自网络,均已备注了出处。 如发现有侵权,请通过邮箱联系我 admin 艾特 crifan.com ,我会尽快删除。谢谢合作。

各种技术类教程,仅作为学习和研究使用。请勿用于任何非法用途。如有非法用途,均与本人无关。

鸣谢

感谢我的老婆**陈雪**的包容理解和悉心照料,才使得我 crifan 有更多精力去专注技术专研和整理归纳出这 些电子书和技术教程,特此鸣谢。

其他

作者的其他电子书

本人 crifan 还写了其他 150+ 本电子书教程, 感兴趣可移步至:

crifan/crifan_ebook_readme: Crifan的电子书的使用说明

关于作者

关于作者更多介绍,详见:

关于CrifanLi李茂 – 在路上

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-06-03 22:04:25

绕过抓包限制概述

移动端(iOS、Android等)的app抓包期间,往往会遇到各种限制。

除了普通的,比如https的SSL证书安装等事情,可以通过安装抓包工具(Charles等)的SSL根证书之外 (举例:移动端安装ssl证书·app抓包利器:Charles),其他还些相对更加高级的,和抓包工具本身独立 的相关内容,可以统称为:绕过抓包限制。

下面就来详细介绍一下,如何绕过这些抓包的限制。

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-06-03 22:03:21

绕过证书绑定

在移动端(iOS、Android等)的app的抓包期间,如果有些https请求,在之前抓包软件已设置了好各种证 书和配置后,看到的:

• 要么是 unknown

• 要么是:加密的乱码

0

• 要么是:报错无法抓包

而无法看到我们希望的明文数据,则:

最大可能是,对方用了https的: SSL pinning

什么是SSL pinning

- SSL pinning = certificate pinning = 证书绑定 = SSL证书绑定
 - 。 原理:
 - 内部加了ssl证书的校验,给合法的有效的证书,先计算出 fingerprint,通过 fingerprint 指纹去匹配对比,才视为有效,否则拒绝访问
 - 效果:对方的app内部,只允许,承认其自己的,特定的证书
 - 导致此处Charles的证书不识别,不允许
 - 导致Charles无法解密看到https的明文数据

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-06-02 10:43:30

Android

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-05-30 17:39:50

信任证书问题

对于 Android 7.0 = API 24 之后,做了些改动,使得系统安全性增加了,导致:

- app 默认不信任用户域的证书
 - -》之前把(Charles 的)ssl证书, 安装到 受信任的凭据 -> 用户 就没用了, 因为不受信任了
 - 。 只信任(安装到)系统域的证书

导致无法抓包https,抓出来的https的请求,都是加了密的,无法看到原文了。

对此,总结出相关解决思路和方案:

- (努力想办法)让系统信任Charles的ssl证书
 - 。 作为app的开发者自己: 改自己的app的配置, 允许https抓包
 - 重要提醒:前提是得到或本身有app的源码
 - 。 把证书放到受系统信任的系统证书中去
 - 重要提示:前提是手机已root

下面详细介绍:

自己修改app去增加配置,允许https抓包

通过修改app的配置,使得允许https抓包

而修改app的配置,又分两种:

- 自己有app源码
 - 。 可以通过修改源码的方式去添加允许https抓包的配置
- 自己没源码,只有apk
 - 。 借助第三方工具修改apk,增加配置,允许https抓包

下面详细介绍如何操作:

通过修改app源码去增加配置允许https抓包

前提:

- 要么你自己是该app的开发者
 - 。本身就有源码,就是app的拥有者
- 要么是你想要破解app的人
 - 。 本身就不可能有源码
 - 但是
 - 如果,有技术,有能力,有运气,破解得到app源码
 那理论上也可以使用此办法
 - 加生化工也可以使用此外况
 - 注意:实际情况下,往往没机会破解出app源码
 - 所以此办法不适用

如果具备修改app的源码,则具体操作过程是:

修改 AndroidManifest.xml , 增加如下配置:

```
<?xml version="1.0" encoding="utf-8"?>
<manifest ... >
<application networkSecurityConfig="@xml/network_security_config"
... >
... >
... >
... >
... >
```

在 res 目录下新建一个 xml 文件夹, 再新建文件:

res/xml/network_security_config.xml

内容为:

手机中已正确安装Charles证书

```
<?rxml version="1.0" encoding="utf-8"?>
<network-security-config>
<domain-config>
<domain includeSubdomains="true">你要抓取的域名</domain>
<trust-anchors>
<certificates src="user"/>
</trust-anchors>
</domain-config>
</network-security-config>
```

其中:

• <certificates src="user"/>: 信任用户自己安装的证书

手机中没安装Charles证书,但是已有Charles证书文件

```
<?rxml version="1.0" encoding="utf-8"?>
<network-security-config>
<domain-config>
<domain includeSubdomains="true">你要抓取的域名</domain>
<trust-anchors>
<certificates src="@raw/证书文件名"/>
</trust-anchors>
</domain-config>
</network-security-config>
```

然后再去:

- res 目录下新建一个 raw 文件夹
 - 。将手机上安装的证书文件放入 res/raw/ 目录下
 - 支持的证书格式: pem , ca

用工具修改apk增加配置允许https抓包

比如借助第三方工具:

levyitay/AddSecurityExceptionAndroid

```
去下载源码,再去:
```

```
cd AddSecurityExceptionAndroid
./addSecurityExceptions.sh //xxx.apk
```

即可给apk增加允许https抓包的配置了,然后就可以继续用Charles抓包https了。

把证书放到系统信任区

- 背景和思路: 既然只信任系统区的证书, 那么可以想办法把Charles证书放到系统区, 就可以被信任 了, 就可以https抓包了

 - 。 而系统信任的地方
 - 对应安卓的设置中的: 受信任的凭据 -> 系统
 - 对应安卓系统目录: /system/etc/security/cacerts/
 - 对应的系统证书的名字有特定规则
 - 需要找到工具根据规则计算出名字后
 - 才能再去把证书放到系统区中
- 前提: 手机已root
- 详细步骤
 - 。 计算证书名

openssl x509 -subject_hash_old -in charles-ssl-proxying-certificate_saved.pem

- 算出数值,比如 3a1074b3
- 。 证书文件改名
 - 然后把原Charles证书 charles-ssl-proxying-certificate_saved.pem 改名
 - 为 3a1074b3.0
- 。 放到系统分区
 - 放到 /system/etc/security/cacerts/
- 注意
 - 。 但是呢, 现在多数手机都很难root了
 - 包括我之前的锤子M1L和很多常见品牌,比如小米、华为等,的最新手机
 - 。 如果真的可以root,那倒是容易此办法去解决ssl pinning的问题

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-05-31 09:52:52

Xposed插件

用其他工具绕开https校验实现https抓包:

- 确保了手机已root
 - Android: 已root
 - 确保后续可以安装 Xposed 等工具
- 再去用可以绕开/禁止 SSL pinning 的插件
 - Android
 - 基于 Xposed 的JustTrustMe
 - 限制:
 - 只能支持 Android 7.0 之前的安卓
 - 超过 Android 7.0 就不工作了
 - 基于 Cydia 的Android-SSL-TrustKiller

即可绕开ssl的验证,抓包到https被解密变成明文的数据。

接下来详细,如何在已 root 的 安卓 中,基于 xposed 框架和相关插件,去实现绕开https证书校验,实 现抓包https得到明文数据。

准备好已root的安卓

对于想要获取已root的安卓,有两种方式:

- 对于安卓 真机 来说
 - 。 很久之前是很简单的事情
 - 随便买个安卓手机,都容易去 root
 - 。 现在
 - 大多数手机品牌(小米,华为等)新买到的都是安卓新版本
 - 比如: Android 8.0 , Android 9.0 之类的
 - 且都很难root
 - 都要向官方申请,要等很长时间(以月为单位)
 - 申请先解锁 BL = BootLoader
 - 然后才能root
 - 而且最后还未必通过
 - 结论就是:
 - 现在很难买到能root的新安卓手机了
 - 。 所以
 - 最终方案是:
 - 去淘宝买个二手的已root的安卓手机
 - 比如:400元左右的
 - 二手小米4
 - 型号: MI 4 LTE-CU
 - 安卓系统版本: Android 4.4.4
- 对于安卓 模拟器 来说

- 。 Mac中也有很多安卓模拟器
 - 目前测试能用的有
 - 夜神Nox 安卓模拟器
 - 模拟的是: Android 4.4.2
 - 网易MuMu 安卓模拟器
 - 模拟的是: Android 6.0.1
 - 其他不能用,不好用的有
 - Andy: 安装后无法正常运行
 - 天天模拟器:没有我要的Mac版
 - Genymotion: 收费的, 还要麻烦的去破解, 暂时懒得继续试
 - BlueStacks:只支持Win,不支持Mac,且也比较老旧

如前所述,已root的安卓,可以选用:

- 安卓真机
 - 。 二手小米4: Android 4.4.4
- 安卓模拟器
 - 。 夜神模拟器: Android 4.4.2
 - ◎ 网易MuMu: Android 6.0.1

中的任何一个。

此处以Mac中的 夜神模拟器 为例去解释。

• Mac版 夜神模拟器 Nox App Player

- 0
- 已经root了

• 模拟的是: Android 4.4.2

o

0

♀ 夜神模拟器

关于夜神的更多解释详见:

好用的安卓模拟器:夜神Nox

安装Xposed框架

在已root的安卓中,安卓Xposed框架。

根据Xposed官网解释,Xposed的版本和安卓版本需要对应,否则无法正常安装和使用:

- Android 4.0.3 ~ Android 4.4
 - 。 用 v2.7 , v2.6.1 的 Xposed installer
 - 支持: 此处基于 Android 4.4.2 的夜神安卓模拟器
- Android 5 以上
 - 。 用 3.x 版本的 Xposed installer
 - 比如: 3.5.1

下面介绍在夜神模拟器中安装Xposed的详细步骤:

下载 v2.7 的xposed installer的de.robv.android.xposed.installer_v33_36570c.apk:



然后拖动到夜神模拟器中,即可自动安装,安装完毕后,可以在桌面上看到:



接着点击进入 Xposed Installer , 再去安装 Xposed框架 到安卓系统中: 点击 安装/更新 , 在弹框中对于 超级用户请求, 设置 永久记住选择 :



然后会去安装到系统中,再点击确定去重启:

• •	•	₩ 夜神安	卓模拟器	\$
ı ش	A 💽			₹1 🖬 4:40
	<♡∑ 框架			
ø	版本:		激活	程序自带
\$	app_process XposedBridge.jar		58 54	58 54
⊲>	框架			
۲×		安装	/更新	
		卸	载	
aék.	安装方式			
20	SD 卡: /storage de.robv.android	/emulated/0/Ar d.xposed.installe	ndroid/data/ er/files	
	正在复制 Xpose 正在挂载 /syste 成功备份于 /sy 正在复制 app_p 正在复制 Xpose	ed-Disabler-Reco em 为可写入 stem/bin/app_p irocess edBridge.jar	overy.zip rocess.orig	- 1
	完成!修改将于	重启之后生效。		
	您现在要重启吗	?		_
	取別	肖		确定
¢				
٦				

重启后,看到Xposed框架中显示:

app_process 激活 58 程序自带 58 XposedBridge.jar 激活 54 程序自带 54

••	•	₩ 夜神安	草模拟器	\$
-	A			📚 🛯 🖬 4:51
	<₽₽ 框架			
ø	uc + .		266-225	印度白井
r1 »	叔本: app_process		湖()古 58	程序目帘 58
7″	XposedBridge.jar		54	54
\$	框架			
د1×		安装/	/更新	
		卸	载	
ape	安装方式			
		经典 (直接写	入 /system)	
	重启			
		软重	启	
		重	启	
4				
L.				
đ				

表示Xposed框架已激活,可以继续使用了。

♀ Xposed框架

关于Xposed框架的更多解释详见:

安卓逆向调试: XPosed框架

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-06-02 10:29:55

用JustTrustMe破解ssl pinning

再去下载和安装 JustTrustMe :

去JustTrustMe的GitHub的release下载JustTrustMe.apk

JustTrustMe.apk de.robv.and...36570c.apk Nox_installe...1.0_cn.dmg MemuInstaller-1.4.4.dmg Andy_46.16_48.dmg

 11 KB

 创建时间
 2018/9/7 16:55

 修改时间
 2018/9/7 16:55

 上次打开时间
 2018/9/7 16:55

 添加标记...

像安装普通安卓apk一样,拖动进去,即可把 JustTrustMe.apk 安装到夜神模拟器中。

注意:此 JustTrustMe 没有app界面,所以安卓后,也没有 打开 之类的操作。而只能是,去Xposed中才 能看到和激活此应用。

然后去Xposed中找到并勾选以激活 JustTrustMe :



然后记得重启Xposed:

• •	•	₩ 夜神:	安卓模拟器	٥
Ċ	▲ 😋 😋 < ⁽ ○ 💁 框架			╤, ₄ 🛿 4:59
© 1	版本: app_process		激活 58	程序自带 58
√ >	XposedBridge.jar 框架	▲ 雷白	54	54
⊲×		▲ 里/□ 您确定?		
	安装方式	取消	确定	
¢	重启			
		ŧ	秋重启	
٥		1	重启	

Charles抓包可以看到https明文

然后再去用Charles抓包:

对于之前没有启动https的,抓包https看到的都是 unknown 的请求和数据是加密的乱码:

•••	Charles 4.2.6 - Session 1 *
Structure Sequence	Overview Contents Summary Chart Notes
Comparison of the second	CONNECT childapi.qupeiyin.com:443 HTTP/1.1 Host: childapi.qupeiyin.com:443 Proxy-Connection: Keep-Alive User-Agent: okhttp/3.11.0
 cunknown> cunknown> thtps://ing.qupeiyin.cn thtps://shence.qupeiyin.cn:8106 sa?project=default sa?project=default sa?project=default https://android.clients.google.com https://play.googleapis.com https://play.googleapis.com thtps://bidapi.guneiy.com 	[@\$J) 6@((īj\i; ÆPbp?[1T`, v]āmi kōwû úÿ: Bêù Ñ®a× © î nĒĀ ā+a 4 2 4 2 4 4 4 4 4 4 4 4 4 4 4 4 4
home 0 refreshModule?sign=4dfc2642c4e2	Headers Text Hex Raw
 Anttps://www.googleapis.com Anttps://cloudconfig.googleapis.com 	Image: Product and examinated Image: Product and examinated and examinated Image: Product
Filter:	Headers Text Hex Raw
POST https://shence.gupeivin.cn:8106/sa?project=de	fault Recording

现在,即可绕开app的https的证书校验,从而可以看到明文数据了:

•••	Charles 4.2.6 - Session 1 *												
	>		1	•	1 C			€ @					
Structure Sequence	Overview	Conten	ts t	Summary	Chart	Notes	5						
 ▼	GET /home/refres HTTP/1.1 Umeng-Cha AREA: 3205 DISTINCT-ID versionCode App-Versior User-Agent: Client-OS: 4 idfa: 864394 Device-Modd Host: childa Connection: Accept-Enco	hModule?s nnel: ying_) : 000EC6F(: 1080 : V5.0.0 android .4.2 d010001412 el: A0001 pi.qupeiyin. Keep-Alive oding: gzip	ign=4d vong_bi C7BBE0	fc2642c4e ao 000	25c098be)db657a	92921c&i	timestamp	=15363113	154&uid=08	kid=1&auth_	_token=0&n	um=4&modu
	Headers 1 {"data ng","t 8","tit 2018- 15:26' u3011 0a.jpg 10:05' u5170 8-06- 16:23' \u6211 me":"2	Query S ":{"id":1", >over":http le!":\\u5f00' 08-31\y5b8 (98-31\y5b8 (98-31\y5b8 (98-31\y5b8 (98-31\y5b8 (98-31\y5b8 (98-31\y5b8 (98-31\y5b8 (98-31\y5b8 (98-31\y5b8 (98-31) (97-31) (tring title":"\ ss:\Vim \u5566 8bafe8 ","data 00\u4e 14541",)","data \u4\u53 0","data \u4\u53 17:58"	Raw (u4eca)u65 g.q.ppeiyin, (u5b63)uff (c38.)g9", [_from":0," [_from":0," [_from":0," [_foot] [_from":0," [50]u4e88", [_solu4e88", []solu488", []solu488", [e5\u66f4\t ccn/2016-(1a\u7406\u views":15 request_idi ff0c\u7ffb request_idi 'https:\Vin request_id' ","jic":"http ","data_fro	65b0"," 1-15\56 60f3\u4 301","cr :"0","is_ u5230\u b6-22 :"0","is_ g.qupei :"0","is_ ss:\Vimg m":0,"re	'snum":"4 59899b75 e2dVS\u7 eate_time collect":C u7b2c20\u collect":C g.qupeiyin equest_id	","icon":" 9d34.png 3b0\u5b9 ":"2018-0 ,"is_unloc 19875","p),"is_unloc 118-09-05),"is_unloc .cn\2018 ":"0","is_c	https:\/\im ","sub_titl le\u4e2d\u 8-29 ck":"1"},{"i ic":"https: csk":"1"},{"i V5b8fa0ff csk":"1"},{"i co9-04/5t collect":0,"	g.qupelyin. *':"", "modu 7684\u4f60 4":"57818", Wimg.qupa 4":"57813", 18329.jpg", 182460e3es s_unlock":'	cn\/2018-0 lle":"courses "rile":"htt "title":"\u32 eiyin.cn\/20 "title":"\u52 "views":"13 "title":\u72 ed.jpg", "vi 1"}]}, "statu	2-24/5a90 *,",course": tps://img.q 210/u5c0f/u 18-09-04/5 3d7/u4f24/u 052","creat ac8/u468e/u ews":"3637 is":1}	e2ddd5f57.p [{"id":"6099 jupeiyin.cn\/ 9e66\u9e49\ 5b8e3db2110 i7684\u5f17\ ie_time":"201 i627e\u5230 5","create_ti
Filter:	Headers	Text	Hex	JavaScri	pt JSC	N J	SON Text	Raw					
CONNECT https://play.googleapis.com													Recording

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-06-02 10:31:15

TrustMeAlready

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-05-30 17:39:50

iOS端

- 前提
 - 。 iOS:已越狱
 - 确保后续能安装 Cydia / Sileo 等包管理器
- 绕过SSL pinning的工具
 - 插件=tweak=越狱插件
 - 最好用的是: NyaMisty/ssl-kill-switch3
 - Repo源地址
 - https://repo.misty.moe/apt/
 - 下载地址
 - https://github.com/NyaMisty/ssl-kill-switch3
 - https://github.com/NyaMisty/ssl-kill-switch3/releases
 - v1.5.1
 - rootfull
 - moe.misty.sslkillswitch3_1.5.1+rootful_iphoneos-arm.deb
 - roothide
 - moe.misty.sslkillswitch3_1.5.1+roothide_iphoneos-arm64e.deb
 - rootless
 - moe.misty.sslkillswitch3_1.5.1+rootless_iphoneos-arm64.deb
 - 注意: 安装后要开启才能使用
 - 设置 -> SSL Kill Switch 3 ->勾选=开启: Disable Certificate Validation



	无 SIM 卡 🗢 🔆	_	上午10:08		• +
	〈 已安装		详情		卸载
		SL Kill Sv 5.1+rootfu	vitch 3		196 kB
	🔅 更改软	次件包设置			>
	🖂 作者	NyaMisty<	misty@mistyn	nce>,Alban[Diquet 🔉
	Blackbox to including ce Apps.	ol to disable rtificate pin	e SSL certifi ning - withir	cate valida i iOS and C	tion - 9S X
	已安装软件包]			
	山 版本			1.5.1+	-rootful
	😑 文件系	系统内容			>
		moe.mi	sty.sslkillswitc ・插件	h3	
■ ● 效果 ■ Wha	atsApp的https请求可	以看到明文	文史	口文衣	技系

https://v.whatsapp.net



- Apple的相关请求也可以看到明文
 - https://gateway.icloud.com.cn

•••																
				> (۵ 🔒	19	0					۲				
Structure	Seque	nce														
Code	Method	Host	Path											Start D	uration Si	ze Status
200		captive.apple.com	/hotspot-detect.html											22:54:25	380 ms	630 bytesComplete
200	POST	gsp85-cn-ssl.ls.apple.com	/wifi_request											22:54:25	664 ms	20.71 KB Complete
200		init.itunes.apple.com	/bag.xml?ix=6&os=13&l	ocale=en_M0											823 ms	73.27 KB Complete
200		gateway.icloud.com.cn:443	/ckdatabase/api/client/z	one/sync										22:54:27		19.88 KBComplete
200	POST	gateway.icloud.com.cn:443	/ckdatabase/api/client/z	one/sync										22:54:27	382 ms	711 bytesComplete
400		gateway.icloud.com.cn	/static/protobuf/CloudDl	3/CloudDBCli	ient.desc									22:54:30		18.17 KBComplete
400		gateway.icloud.com.cn	/static/protobuf/CloudDI	3/CloudDBCli												1.66 KBComplete
200		gsp64-ssl.ls.apple.com	/hvr/v3/use											22:54:36		15.88 KBComplete
301		superman.host	/api/ios/req													665 bytes Complete
200	CONNECT	superman.host												22:54:42		524 bytesComplete
200	CONNECT	superman.host														524 bytesComplete
200	CONNECT	superman.host												22:54:44		157 bytes Complete
400		gateway.icloud.com.cn	/static/protobut/CloudDl	B/CloudDBCli												18.18 KB Complete
400		gateway.icloud.com.cn	/static/protobuf/CloudDl	3/CloudDBCli	ient.desc									22:54:58		18.17 KB Complete
Filter																Focused Settinge
																C rocado Couriga
Overview	Conte	nts Summary Chart	Notes													
IO exception https://gate	in retrieving eway.icloud	the descriptor file from 'http: .com.cn:443/static/protobuf/C	s://gateway.icloud.com.cn CloudDB/CloudDBClient.de	443/static/p ic	protobuf/C	loudDB/	CloudDBCli	ent.desc'	: Unexpect	ed respo	onse co	de '400' re	ceived from:			Settings
1 { 2: "com. 3: "com. 7 { 1: "C0 2: 2	apple.reni apple.reni 18AA7ED-714	nders" nders" 10-4ADD-9315-1467F95E61DA"														
Headers	Text	Hex Compressed Pr	otobuf Protobuf Text	Raw												
server: App date: Fri, 21 content-ty x-respondii content-en strict-trans x-apple-xra x-apple-ret x-apple-ret access-con x-apple-ret C + \$2228763A	oleHttpServo 0 Oct 2023 pe: applicat ng-instance coding: gzi port-securi ail: true er-partition oud-xrail-gi quest-uuld: atrol-exposis ge-respons	eyr686669120c64 1458-27 0KT ion/x-protobuf c: ckdstabaseservice:10599725 p ty: max-age=31536000; includ: 2:12 roup234-ext-79958dbc-hwi6 00292655-0824-338.A 750- badder: X-Apple-Request-L e-time:56 5-9644-78471C154DA8 E	584:prod-p212-ckdatabas deSubDomains; k:8301:238446:grp234,eff JUID,Via	2567vice-100 5195d8621b	Dpercent-7 e56114387	19c9d6; 7549e174	785-rzc9b:8 ce198:4f38i	8080:232 8eba840t	6B351:4b2 bab1ef61e7;	od282d3	3091e91 '953:xar	la14ad04f6 ctu2	i9ec48a3bcd06	667		
Headers				Raw												
GET https://g	ateway.icloux	.com.cn/static/protobuf/CloudDB/Cl	oudDBClient.desc													Block List Recording

- 其次是: evilpenguin/SSLBypass
 - 下载地址
 - https://github.com/evilpenguin/SSLBypass
 - https://github.com/evilpenguin/SSLBypass/blob/main/packages/com.evilpengui n.sslbypass_1.0-5%2Bdebug_iphoneos-arm.deb
 - 插件详情



https://github.com/nabla-c0d3/ssl-kill-switch2

- https://github.com/nabla-c0d3/ssl-kill-switch2/releases
 - https://github.com/nabla-c0d3/ssl-killswitch2/releases/download/0.14/com.nablac0d3.sslkillswitch2_0.14.deb

■ 插件详情

No SIM 奈	2:57 PM	
Installed	Details	Remove
SSL 0.14-	Kill Switch 2 3+debug	84 kB
Change	Package Setting	gs 🔉
Author		Alban Diquet 🔉
Blackbox tool to including certifi Apps.	o disable SSL certif cate pinning - withir	icate validation - n iOS and OS X
INSTALLED PAC	CKAGE	
Version		0.14-3+debug
E Filesyste	em Content	>
C	om.nablac0d3.sslkillsv · Tweaks	vitch2
Cydia Sour	ces Changes	Installed Search
■ 注: ■ 旧版本:iOS SSL Kill Swi	tch	

■ 其他

- SSL Kill Switch 2 (iOS 13)
- ∘ Frida 的jS
 - 绕过证书校验
 - Frida CodeShare Project: iOS SSL Bypass

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-06-02 10:35:18

插件

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-05-30 17:39:50

SSL Kill Switch

记得是有多个版本:

- SSL Kill Switch 2
- ssl-kill-switch3

抓包举例

SSL Kill Switch 2 (iOS 13)

Apple账号

经测试, Apple账号登录过程中的https请求:

- 除了特殊的,特定的:
 - https://gsa.apple.com
- 之外,其他普通的(包括带账号绑定的https请求),是可以抓包的,能看到明文的
 - 。 比如:
 - https://setup.icloud.com
 - https://bag.itunes.apple.com

具体步骤:

- 手机
 - 。 iPhone8: iOS 15.1 、 palera1n 的 rootful 越狱
- Sileo中安装插件
 - julioverne 的 SSL Kill Switch 2 (iOS 13)
 - 源地址: https://julioverne.github.io

编辑	Sileo - 粘贴自:微信	+
软件	牛源	
	所有软件包 查看已经添加的软件源的所有软件包	84 >
软件	添加1个软件源	
BB	添加以下从剪贴板中找到的 URL : https://julioverne.github.io/	1 >
R	添加1个软件源	1 >
	手动输入	4 >
	取消 nttps://repo.paiera.in/	2 >
	palera1n strap https://strap.palera.in/	66 >
5 软件源		
大 精选	 ・ ・	Q 搜索



无SIM卡 🗢	下午 3:17	100% 🛃
< 返回	已安装的文件	
• /		
▼ Li	brary/	
•	MobileSubstrate/	
	 DynamicLibraries/ 	
	SSLKillSwitch2.dylib	
	SSLKillSwitch2.plist	
•	PreferenceLoader/	
	 Preferences/ 	
	SSLKillSwitch.png	
	SSLKillSwitch_prefs.plist	



精选







搜索

https抓包效果:

- 能抓包明文的
 - https://bag.itunes.apple.com/bag.xml

Structure			
Structure		> • ≟ A ● 🥖 C 🗸 🔀 ⊗	
	Sequence		
Code	Method Host	Path Start Duration Size Status Info	
200	POST sp1.baidu.com	/5b1ZeDe5KgQFm2e88luM_a/webb.gif?pid=4_145&lid=109819099461417 15:22:51 20 ms 1.45 KBComplete	
200	POST sp1.baidu.com	/5b1ZeDe5KgQFm2e88luM_a/webb.gif?pid=4_145&lid=109819099461417 15:22:51 63 ms 28.37 KBComplete	
0 200	POST mbd.baidu.com	/ztbox?action=zpblog&appname=baiduboxapp&v=2.0&data=%7B%22cateid 15:22:51 75 ms 29.36 KBComplete	
200	CONNECT captive.apple.com	15:22:54 1.09 s 36.42 KBComplete	
Filmer			Facurad Cat
Pilter:			Focused Set
x-apş x-apple-clit	accept */* ile-store-front 143441-19,29 int-application com.apple.Preferences		
if-i acc	x-apple-tz 28800 nodified-since Tue, 04 Jul 2023 03:33: user-agent com.apple.Preferences/1 :ept-language zh-Hans-CN	32 GMT I ICS/150 model/Phone10,1 hwp/t8015 build/19A346 (6; dt:157) AMS/1	
if-I acc Headers	x-apple-tz 28800 modified-since Tue, 04 Jul 2023 03:33: user-agent com.apple.Preferences/1 :ept-language zh-Hans-CN Query String Cookies Raw	32 GMT I OS/15.0 model/iPhone10,1 hwp/t8015 build/19A346 (6; dt:157) AMS/1	
if-I acc Headers	x-apple-tz 28800 modified-since Tue, 04 Jul 2023 03:33: user-agent com.apple.Preferences/1 :ept-language zh-Hans-CN Query String Cookies Raw :status 304	32 GMT 1/GS/15.0 model/iPhone10,1 hwpt8015 build/19A346 (6; d: 157) AMS/1	
if-i aci Headers	x-apple-tz 28800 modified-since Tue, 04 Jul 2023 03:33: user-agent com.apple.Preferences/1 :ept-language zh-Hans-CN Query String Cookies Raw :status 304 date Tue, 04 Jul 2023 07: Jacornelation.exu DN 126429/VCEED44	32 GMT 1/05/15.0 model/iPhone10,1 hwp/t8015 build/19A346 (6; dt:157) AMS/1 23:05 GMT 23:05 GMT	
if-ı acı Headers x-apple-jing x-aj	x-apple-tz 28800 war-agent com.apple.Preferences/I user-agent com.apple.Preferences/I user-agent com.apple.Preferences/I verget-language zh-Hans-CN Query String Cookies Raw :status 304 date Tue, 04 Jul 2023 07: le-correlation-key RNJ7&SX3YVEF5P4I sple-request-uold BbS304a-bc5-485	32 GMT I I GS/15.0 mode/liPhone10,1 hwp/t8015 build/19A346 (6; dt:157) AMS/1 :23:05 GMT JHBUA7WUM -eH93-360346/edd43	
if-∴ acu Headers x-apple-jing x-aj	x apple-tz 28800 modified -since Tue, 04 Jul 2023 03:33: user-agant com apple-Preferences/T sept-language zh-Hans-CN date Tun, 04 Jul 2023 07: le-correlation-key RNJ7ASX3YVEFSP4U ple-request-uuid bb5704abc5488eb b 3 bb5304abc5488eb	32 GMT 1/GS/15.0 mode/l/Phone10,1 hwp/t8015 build/19A346 (6; d: 157) AMS/1 22:06 GMT DHIBU47WUIM e-bf83-3a034r2ed443-1dbbf43f8f466arf9	
if- acı Headers x-apple-jing x-aj	x apple-tz 28800 wiese-agent com apple-preferences/f suser-agent com apple-Preferences/f sept-language S-h-Inan-CN Query String Cookies Raw istatus 304 date Tue, 04 Jul 2023 07; le-correlation-kay RNJ7ASX3VYEF594J le-correlation-kay RNJ7ASX3VYEF594J b3 6b53704abc5486b b3 36b53704abc5486b	32 GMT 11G5/15.0 model/Phone10,1 hwp(t8015 build/19A346 (6; d:157) AMS/1 23:05 GMT DHEUL47VUIM 4-1653-3403467ed443 183300347ed443-10bt/318/466e19 183300347ed443	
if- acı Headers x-apple-jing x-aj	x-apple-tz 28800 modified-since two, 04 Jul 2023 03:33: user-agent com.apple-Preferences/r espl-language 24-hans-CN Query String Cookies Raw :status 304 date Tue, 04 Jul 2023 07: le-correlation-kay RNJ7AS/31VEF5041 pple-request-uuid 855104_a-hot5-485 b3 8b53104antc54886 x-b3-spanid 1bb/d43181666af9	32 GMT 1 IOS/15.0 model/iPhone10,1 hwp/t8015 build/19A346 (6; dt:157) AMS/1 23:05 GMT DHIBUATWIM HH33a034e7e4d43 1#33a034e7e4d43	
if- acı Headers x-apple-jing x-aj	x-apple-tz 28800 modifide-ince tvo, 04 Jul 2023 03:33: user-agant com.apple-Preferences/ capt-language zh-Hans-CN Query String Cookles Raw istatus 304 date Tun, 04 Jul 2023 07: le-correlation-key RNJ7ASX3YVEFS4U pple-request-uuid ab5/304.abc5435eb x-b3-apal-tab64364 x-b3-traceid ab5/304.abc5435eb x-b3-apale data/abd643f8466459 apple-seq 0.0	32 GMT 1IGS/15.0 mode/l/Phone10,1 hwp/t8015 build/19A346 (6; d: 157) AMS/1 22:06 GMT DHIBU47WUIM e-M58-3-8034e7ed443 18330034e7ed443	
if- ac: Headers x-apple-jing x-aj	x-apple-tz 28800 washer to da ut 2023 03:33: user-agent com.apple-Preferences/ ept-language 2-hana-CN Query String Cookies Raw istatus 304 date Tuo, 04 Jul 2023 07: le-correlation-kay RNJ7ASX3YVEF5944 jel-request-uud 8b5304a-fc-56-865 b3 8b5304afc-56-865 x-8-3-randi dbb/33f6466819 apple-tk faise Paw	32 GMT 1 I GS/15.0 model/IPhone10,1 hwp/t8015 build/19A346 (6; d: 157) AMS/1 :23:05 GMT DHIBUR7WUM = +0583-38034e7ed443 1833a034e7ed443 - 10bbf4318/1466a19 1833a034e7ed443	
if- acı Headers x-apple-jing x-aj Headers	x-apple-tz 28800 washing status (p. 04 Jul 2023 03:33: user-agent com.apple.Preferences/ ept-language zh-Inan-CN Query String Cookles Raw :status 304 date tw. 04 Jul 2023 07: de-correlation-key RNJ7ASX3YVEF5P4J pathe-request-uuid BbS3104.ahc564866 x-b3-traceld BbS3104ahc5648666 x-b3-traceld BbS3104ahc5648666 x-b3-traceld BbS3104ahc5648666 x-b3-traceld BbS3104ahc5648666 x-b3-traceld BbS3104ahc5648666 x-b3-traceld BbS3104ahc5648666 x-b3-traceld BbS3104ahc5648666 x-b3-traceld BbS3104ahc56486667 apple-seq 0.0 apple-tz 200	32 GMT 1 IGS/15.0 model/iPhone10,1 hwp/t8015 build/19A346 (6; d: 157) AMS/1 :23:05 GMT DHIBUA7WUM e-H873-3603467ed443 1833e034e7ed443-1dbbf43f8f466af9 1833a034e7ed443	
if- ac: Headers x-apple-jing x-a X-apple-jing x-a Ger https://bu S://Se	x-apple-tz 28800 modifide -ince two, 04 Jul 2023 03:33: user-agent com.apple-Preferences/ ept-language 24-hans-CN Query String Cookies Raw istatus 304 date two, 04 Jul 2023 07: de-correlation-kwy RNJ7AS/31VEF6741 pple-feeuest-uuid B653704-arbc54856 x-03-spanid tbbd/arbc54856 x-03-spanid tbbd/arbc54856 x-03-spanid tbbd/arbc54856 x-03-spanid tbbd/arbc54856 x-03-spanid tbbd/arbc54856 x-03-spanid tbbd/arbc54856 x-03-spanid tbbd/arbc54856 x-03-spanid tbbd/arbc54856 x-03-spanid tbbd/arbc64856 x-03-spanid tbbd/arbc64856 x-03-spanid tbbd/arbc64856 x-03-spanid tbbd/arbc64856 x-03-spanid tbbd/arbc64856 x-03-spanid tbbd/arbc46856 x-03-spanid tbbd/arbc64856 x-03-spanid tbbd/arbc46856 x-03-spanid tbbd/arbc468	32 GMT 105/15.0 model/iPhone10,1 hwp/t8015 build/19A346 (6; dt:157) AMS/1 23:05 GMT 23:05 GMT DHIBUA7WUM 105/15/0 model/iPhone10,1 build/19A346 (6; dt:157) AMS/1 1833a03407ed443-1cbuild/316/466a19 1833a03407ed443 mm&format-ison&os=05&os=15.0&product-com.apple.Preferences&product/Version=1&profile=VideoSubscriberAccount&profile/Version=1&storefront=143441-19,29 /Setup/qulify/Session	Ro
If- ac Headers x-apple-Jing X-a X-apple-Jing X-a GET https://bc	x-apple-tz 28800 modified-ince two, 04 Jul 2023 03:33: user-agent com.apple-Preferences/ epit-language 24-hane-CN Query String Cookies Raw istatus 304 date two, 04 Jul 2023 07: de-correlation-kwy RNJ7ASX3VVEF6941 pple-request-uuid B653704-arbc54856 x-03-apple-stq 0.0 apple-stq 0.0 apple-st false Raw g itunes apple combag xm?deviceClass=IPF	32 GMT 105/15.0 model/iPhone10,1 hwp/t8015 build/19A346 (6; dt:157) AMS/1 :23:05 GMT DHBUA7WUM INF: bHS -3803467ed433 1833a03467ed443 1833a03467ed443 1833a03467ed443 Interferences&product/version=1&profile=VideoSubscriberAccount&profile/Version=1&storefront=143441-19,29 /Setup/qulify/Session Charles 4.6.3b2 - Session 1*	Ro
If- ac Headers x-apple-jing x-a at https://se)S://Se	x-apple-tz 28800 modified-since two, 04 Jul 2023 03:33: user-agent com.apple-Preferenceyl' epit-language x-htmar-CN Ouery String Cookies Raw ise-correlation-key RU/XSX3YVEF6741 le-correlation-key RU/XSX3YVEF6741 ight-request-uuid 8b3704a-htc-54866 x-b3-traced x-b4866 x-b3-traced 8b3704a-htc-54866 x-b3-traced x-b4866 x-b3-traced x-b4766 x-b3-traced x-b4866 x-b3-traced x-b4766 x-b	32 GMT 1105/15.0 model(Phone10,1 hwpt8015 build/19A346 (6; d::157) AMS/1 23:05 GMT 24:05 GMT 24:	Re

			🕨 💌 🛥 🛎 🦉 C	×	× ©				
Structur	e Seque	ence							
Code	Method	Host	Path	Start	Duration	Size Status	Info		
200	POST	sp1.baidu.com	/5b1ZeDe5KgQFm2e88luM_a/webb.gif?pid=4_145&lid=10981909946141	7 15:22:5	20 ms	1.45 KBComplete			
200	POST	sp1.baidu.com	/5b1ZeDe5KgQFm2e88luM_a/webb.gif?pid=4_145&lid=10981909946141	7 15:22:5	63 ms	28.37 KBComplete			
200	POST	mbd.baidu.com	/ztbox?action=zpblog&appname=baiduboxapp&v=2.0&data=%7B%22cate	id 15:22:5	1 75 ms	29.36 KBComplete			
200	CONNECT	Captive.apple.com		15:22:54	1.09 s	36.42 KBComplete			
304	GET	bag.itunes.apple.com	/bag.xml?deviceClass=iPhone&format=json&os=iOS&osVersion=15.0&pro	d 15:23:0	5 133 ms	28.20 KBComplete			
200	GET	setup.icloud.com	/setup/qualify/cert?ver=P1.36.0	15:24:03	419 ms	47.02 KBComplete			
200	GET	setup.icloud.com	/setup/qualify/session	15:24:03	251 ms	1.26 KBComplete			
10.00									0
-liter:								Pocused	Settings
Overview	V Conte	ents Summary Chart Notes							
		GET /setup/qualify/session HTTP/1.1							
	Host	t setup.icloud.com							
-Apple-I	Client-Time	2023-07-04T07:24:03Z							
X-	Apple-I-MD	AAAABQAAABArbf/lutSh9U4INpZ/75MBAA	AAAw==						
X-MMe	-Client-Info	iPhone10,1> <iphone os;15.0;19a346=""></iphone>	<com.apple.appleaccount (com.apple.preferences="" 1.0="" 1109.1)=""></com.apple.appleaccount>						
X-Ap	ple-I-MD-M	uuJ2boSsQdA4ywxQL4cVLXHfVFnGpfTQ7	yMWZ5K7Z/uPN8cdR4Z033zGHuUf48deqfcw3WvUYLNZVIJI						
X-Apple	-I-TimeZone	GMT+8							
X-MMe-	Nas-Session	AQhLLJFIHZt9oGQLK9xT0BluCQrjtQkIUo	Y7D9URKkHFa+YmaQdsajtPuJ8cNCY8/1CBIMxuGGdcLLQLGgFpxixJvgdWJLF	19bVF+nhSsal	IDlembhGTsZ	FbZNoE+/R4hhJuljil+OrR	xiBfLI6UmoV9dVNMeOp	Lyfd49kpj7dMdvD	eKTuhozZM
X-Apple-	I-MD-RINFO	50660608							
X-Ap	ple-I-Locale	∋ zh_CN							
	User-Agent	t %E8%AE%BE%E7%BD%AE/1109.1 CFNet	work/1312 Darwin/21.0.0						
	Connection	1 keep-alive							
Headers	Daw								
Headers	Raw								
Headers	Raw								
Headers	Raw s": true, n-info": "A	AqyzaxbnjwwXMmwmy2jIM48AAABAr6KTGHGL	2Vc44ASkugBL+KPKpCKWvCPerSzdrDwusIxdAf6Nd8szg7ggD8CRQ7QBLhVUn†fN	KxDK/AN8YIF	VyqETOnVsEM	2NB098JpGrftl+4v+NxQA	AADYEBW+AONlhFIJOwa5	8xT13hHpko8kUk	\jA8dXP0lwF
Headers "succes "sessio	Raw s": true, n-info": "/	AgyzaxbnjwwXMmwmy2jIM48AAABAr6KTGHGL	2Vc44ASkugBL+KPkpCkWvCPerSzdrDwusIxdAf6Nd0szg7qqD8CRQ7Q8LhVUnjfN	KxDK/AN8YIF	VygETOnVsEM	2NB098JpGrftl+4v+N×QA	AADYEBW+AON1hFIJOwa5	58xT13hHpko8kUka	\jA8dXPOlwP
Headers "succes "sessio	Raw s": true, n-info": "/	AgyzaxbnjwwXMmwnyZjIM48AAABAr6KTGHGL	2Vc44ASkugBL+KPkpCkWvCPerSzdrDwusIxdAf6Nd6szg7qqDBCRQ7QBLhVUnjfN	KxDK/AN8YIF	VygETOnVsEM	2NBO98JpGrftl+4v+NxQA	AADYEBW+AONlhFIJOwaS	58xT13hHpko8kUk	Nj A8dXPOlwF

• 无法抓包的

•

• https://gsa.apple.com

Headers Text Hex JavaScript JSON JSON Text Raw GET https://setup.icloud.com/setup/qualify/session

Recording

•••			Charles 4.6.3b2 - Session 1 *	× >					
Structure	Seque	ence							
Code	Method	Host	Path	Start [uration	Size Status	Info		
200	POST	sp1.baidu.com	/5b1ZeDe5KgQFm2e88luM_a/webb.gif?pid=4_145&lid=109819099461417.	15:22:51	20 ms	1.45 KBComplete			
200	POST	sp1.baidu.com	/5b1ZeDe5KgQFm2e88luM_a/webb.gif?pid=4_145&lid=109819099461417.	15:22:51	63 ms	28.37 KBComplete			
200	POST	mbd.baidu.com	/ztbox?action=zpblog&appname=baiduboxapp&v=2.0&data=%7B%22cateic	15:22:51	75 ms	29.36 KBComplete			
200	CONNECT	captive.apple.com		15:22:54	1.09 s	36.42 KBComplete			
304	GET	bag.itunes.apple.com	/bag.xml?deviceClass=iPhone&format=json&os=iOS&osVersion=15.0∏	15:23:05	133 ms	28.20 KBComplete			
200	GET	setup.icloud.com	/setup/qualify/cert?ver=P1.36.0	15:24:03	419 ms	47.02 KBComplete			
200	CONNECT	setup.icioud.com	/setup/duality/session	15:24:03	251 ms	20.09 KBComplete			
ilter: Overview troxy-Conne Conne Headers	Conte COP Host gsa. ection kee ection kee	nts Summary Chart Notes NRECT gaa apple.com: 443 HTTP/1.1 apple.com p-alive p-alive						Focused	Settin
HTTP/1.1 2	200 Connec	tion established							
HTTP/1.1 2 Headers	Raw	non established							Report
HTTP/1.1 2 Headers 3ET https://se	Raw etup.icloud.c	tion established							Record
HTTP/1.12 Headers GET https://se http 200 CON gSa T114	tps: NNEC	om/vertup/qualify/session //gsa.apple.co CT pple.com	m						Record
HTTP::/.12 Http://.12 Http:// Http:// Http:// Http:// COP gsa Tue 103	Raw tps: NNEC a.ap e Ju 31	om/setup/gualfy/session //gsa.apple.co CT ople.com NI 04 15:24:43	m CST 2023						Record
HTTP:/.12 Headers htt 200 CON gsa Tue 103 205	Raw http: Stup: St	om/setup/gualfy/session //gsa.apple.co CT ople.com Al 04 15:24:43	m CST 2023						Record
HTTP:/.12 Headers Att http: 200 CON gs& Tue 103 201 Con	tps: NNEC a.ap g l s a.ap g l s a.ap g l s a.ap c s a.ap	on/setup/qualify/session //gsa.apple.co CT ople.com Il 04 15:24:43	m CST 2023						Recor

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-06-02 10:36:13

SSLBypass

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-05-30 17:58:03

其他特殊处理

对于其他更加复杂的特殊情况,一般是:

- 特定的app,内部加了额外的反扒方面的技术手段
 - 。解决方案:往往要涉及到, app的破解和逆向,找到关键点函数,才能针对性的去绕过处理
 - 注:关于app的逆向破解,详见
 - Android逆向开发
 - iOS逆向开发

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-06-02 10:37:19

抖音

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-05-30 17:39:50

Android版

Android版=安卓版抖音,对于网络抓包做了限制,导致的现象是:

• 当已设置好WiFi的代理,再去抓包抖音,会出现: 网络错误。当前无网络,请检查后重试。



0

• mitmdump等抓包工具抓包时报错: Client TLS handshake failed

[16:07:30.334][192.168.1.20:40974] server connect polaris.zijieapi.com:443 (223 111.245.248:443 [16:07:30.381][192.168.1.20:40974] Client TLS handshake failed. The client does not trust the proxy's certificate for polaris.zijieapi.com (OpenSSL Error([('S SL routines', '', 'ssl/tls alert certificate unknown')])) [16:07:30.381][192.168.1.20:40974] client disconnect [16:07:30.381][192.168.1.20:40974] server disconnect polaris.zijieapi.com:443 (223.111.245.248:443) [16:07:33.674][192.168.1.20:40984] client connect [16:07:33.693][192.168.1.20:40984] server connect api3-normal-c.amemv.com:443 ([2409:8c20:aa51:2e:3::3de]:443) [16:07:33.734][192.168.1.20:40984] Client TLS handshake failed. The client does not trust the proxy's certificate for api3-normal-c.amemv.com (OpenSSL Error([('SSL routines', '', 'ssl/tls alert certificate unknown')])) [16:07:42.408] [192.168.1.20:37932] server disconnect i.snssdk.com:443 ([2409:8c 20:5223:104:3::3fd]:443) [16:07:44.161][192.168.1.20:37946] client connect [16:07:44.195][192.168.1.20:37946] server connect log.snssdk.com:443 ([2409:8c2 0:9c73:103:3::9]:443) [16:07:44.321][192.168.1.20:37946] Client TLS handshake failed. The client does not trust the proxy's certificate for log.snssdk.com (OpenSSL Error([('SSL rou tines', '', 'ssl/tls alert certificate unknown')])) [16:07:44.324][192.168.1.20:37946] client disconnect [16:07:44.326][192.168.1.20:37946] server disconnect log.snssdk.com:443 ([2409: 8c20:9c73:103:3::9]:443) [16:07:44.378][192.168.1.20:37962] client connect [16:07:44.403][192.168.1.20:37962] server connect log.snssdk.com:443 ([2409:8c2 0:9c73:103:3::8]:443) [16:07:44.451][192.168.1.20:37962] Client TLS handshake failed. The client does not trust the proxy's certificate for log.snssdk.com (OpenSSL Error([('SSL rou tines', '', 'ssl/tls alert certificate unknown')]))

[16:07:44.453][192.168.1.20:37962] client disconnect [16:07:44.454][192.168.1.20:37962] server disconnect log.snssdk.com:443 ([2409: 8c20:9c73:103:3::8]:443) [16:07:47.372][192.168.1.20:41272] client connect [16:07:47.382][192.168.1.20:41272] server connect i.snssdk.com:443 ([2409:8c20: 5223:104:3::3fe]:443) [16:07:47.412][192.168.1.20:41272] Client TLS handshake failed. The client does not trust the proxy's certificate for i.snssdk.com (OpenSSL Error([('SSL routi nes', '', 'ssl/tls alert certificate unknown')])) [16:07:47.413][192.168.1.20:41272] client disconnect [16:07:47.413][192.168.1.20:41272] server disconnect i.snssdk.com:443 ([2409:8c 20:5223:104:3::3fe]:443)

4

F

主要是用的另外一个手段:

改用另外一个网络库(Google开发的): Cronet

而其默认不允许https抓包,而想要绕过限制,可以去hook特定的一些函数,从而实现,绕过抓包限制,可以正常(https)抓包。

而实现绕过安卓版抖音的抓包限制的:

- 核心思路,就一种
 - hook函数 SSL_CTX_set_custom_verify , 使其参数 mode 从 1 改为 0
 - 目的:实现忽略SSL协议验证,从而允许https抓包

不过具体实现做法=方式,有2种:

- hook代码的方式
 - 。用Frida找到并去hook函数 SSL_CTX_set_custom_verify, 使其参数 mode 从 1 改为 0
- 修改并替换so库的方式
 - 已知上述几个特定函数是属于 libsscronet.so ,所以可以去修改此so库文件,并替换掉该库文 件

下面详细解释:

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-06-02 11:44:40

Frida去hook代码的方式

Frida的hook代码=函数:

hookNative_SSL_CTX_set_custom_verify

```
function hookNative_SSL_CTX_set_custom_verify(){
 var origFuncPtr_verify = Module.findExportByName("libsscronet.so", "SSL_CTX_set_custo")
m_verify");
 console.log("origFuncPtr_verify=" + origFuncPtr_verify)
  // https://commondatastorage.googleapis.com/chromium-boringssl-docs/ssl.h.html#SSL_VE
RIFY_NONE
 // OPENSSL_EXPORT void SSL_CTX_set_custom_verify(SSL_CTX *ctx, int mode, enum ssl_ver
ify_result_t (*callback)(SSL *ssl, uint8_t *out_alert));
 var func_verify = new NativeFunction(origFuncPtr_verify, 'pointer', ['pointer', 'int',
 console.log("func_verify=" + func_verify)
 var newFuncPtr_verify = new NativeCallback(
    function (ctx, mode, callback) {
      console.log("SSL_CTX_set_custom_verify calling: ctx=" + ctx + ", mode=" + mode
", callback=" + callback)
     // #define SSL_VERIFY_NONE 0x00
      // #define SSL_VERIFY_PEER 0x01
      // #define SSL_VERIFY_FAIL_IF_NO_PEER_CERT 0x02
      // #define SSL_VERIFY_PEER_IF_NO_OBC 0x04
     const SSL_VERIFY_NONE = 0
      return func_verify(ctx, SSL_VERIFY_NONE, callback)
      // return func_verify(ctx, mode, callback)
   },
    'pointer',
    ['pointer', 'int', 'pointer']
 console.log("newFuncPtr_verify=" + newFuncPtr_verify)
 Interceptor.replace(origFuncPtr_verify, newFuncPtr_verify)
}
function afterLibLoaded_libsscronet(libraryName) {
 console.log("libraryName=" + libraryName)
 hookNative_SSL_CTX_set_custom_verify()
}
function hookNative_libsscronet(){
 // let libsscronet_so_name = "libsscronet.so"
 // console.log("libsscronet_so_name=" + libsscronet_so_name)
 // FridaAndroidUtil.waitForLibLoading(libsscronet_so_name, afterLibLoaded_libsscronet)
 FridaAndroidUtil.hookAfterLibLoaded("libsscronet.so", afterLibLoaded_libsscronet)
}
function hookDouyin_Native(){
 hookNative_libsscronet()
```

```
function hookAndroid() {
    if( Java.available){
        console.error("Java is not available")
        return
    }
    console.log("Java is available")
    console.log("Java.androidVersion=" + Java.androidVersion)
    Java.perform(function () {
        hookDouyin_Native()
        console.log("----- Begin Hook -----")
    })
    setImmediate(hookAndroid)
```

相关代码:

```
class FridaUtil {
 // Frida pointer to C string
  static ptrToCStr(curPtr){
  var curCStr = curPtr.readCString()
   // console.log("curCStr=" + curCStr)
   return curCStr
 }
}
class FridaAndroidUtil {
  static waitForLibLoading(libraryName, callback_afterLibLoaded){
    console.log("libraryName=" + libraryName + ", callback_afterLibLoaded=" + callback_
afterLibLoaded)
    var android_dlopen_ext = Module.getExportByName(null, 'android_dlopen_ext')
    console.log("android_dlopen_ext=" + android_dlopen_ext)
    if (null == android_dlopen_ext) {
     return
    }
    Interceptor.attach(android_dlopen_ext, {
      onEnter: function (args) {
        // android_dlopen_ext(const char *_Nullable __filename, int __flags, const andr
oid_dlextinfo *_Nullable __info)
        // console.log("args=" + args)
        var filenamePtr = args[0]
        var libFullPath = FridaUtil.ptrToCStr(filenamePtr)
```

```
// console.log("libFullPath=" + libFullPath)
        // var flags = args[1]
        // var info = args[2]
        // console.log("android_dlopen_ext: [+] libFullPath=" + libFullPath + ", flags=
" + flags + ", info=" + info)
       // if(libraryName === libFullPath){
        if(libFullPath.includes(libraryName)){
          console.log("+++ Loaded lib " + libraryName)
          this.isLibLoaded = true
       }
      },
     onLeave: function () {
       if (this.isLibLoaded) {
        callback_afterLibLoaded(libraryName)
          this.isLibLoaded = false
       }
      3
 }
  static hookAfterLibLoaded(libName, callback_afterLibLoaded){
   console.log("libName=" + libName)
   FridaAndroidUtil.waitForLibLoading(libName, callback_afterLibLoaded)
  }
```

最新 (FridaAndroidUtil 等) 工具类函数代码,详见:

https://github.com/crifan/JsFridaUtil/blob/main/frida/FridaAndroidUtil.js

hook输出效果:

```
----- Begin Hook -----
+++ Loaded lib libsscronet.so
libraryName=libsscronet.so
origFuncPtr_verify=0x79d2692fb0
func_verify=0x79d2692fb0
newFuncPtr_verify=0x7d4616e0b8
SSL_CTX_set_custom_verify calling: ctx=0x7b8c2b2f78, mode=1, callback=0x79d13ce5b8
SSL_CTX_set_custom_verify calling: ctx=0x7b8c2e5bf8, mode=1, callback=0x78ecb1d038
SSL_CTX_set_custom_verify calling: ctx=0x7b8c30b718, mode=1, callback=0x78ecb1d038
SSL_CTX_set_custom_verify calling: ctx=0x7b8c307ed8, mode=1, callback=0x78ecb1d038
SSL_CTX_set_custom_verify calling: ctx=0x7b8c2fe8d8, mode=1, callback 0x78ecb1d038
SSL_CTX_set_custom_verify calling: ctx=0x7b8c307258, mode=1, callback 0x78ecb1d038
SSL_CTX_set_custom_verify calling: ctx=0x7b8c321838, mode=1, callback=0x78ecb1d038
SSL_CTX_set_custom_verify calling: ctx=0x7b8c25ec98, mode=1, callback=0x78ecb1d038
SSL_CTX_set_custom_verify calling: ctx=0x7b8c3036f8, mode=1, callback=0x78ecb1d038
SSL_CTX_set_custom_verify calling: ctx=0x7b8c2ceb38, mode=1, callback=0x78ecb1d038
```

	frida -U -f com.s	ss.android.ugc.awem	e -l hook_douyin.js				て第1
mitmwe • #1 ~ (-zsh) #2/DouYin/d #3g/frida/ • #4	g/frida/ 🔵 #5	g/frida/ • #6	g/frida/ 🔵 %7	g/frida/fri %8	g/frida/f 🔵	g/frida/frid	frida (Pyth %9 +
Last login: Mon Aug 26 17:23:58 on ttys036							
→ ~ cd /Users/crifan/dev/dev_root/androidReverse		dynamicDebug/frida	/frida			-custom_verify 28/28	$3 \otimes \langle \rangle \times$
▶ frida frida -U -f com.ss.android.ugc.aweme -l hook_douyin.js		-					
/ _ Frida 16.4.8 - A world-class dynamic instrumentation toolki							
> _ Commands:							
object? -> Display information about 'object'							
exit/auit -> Exit							
More info at https://frida.re/docs/home/							
Connected to M2101K9C (id=9C181A8D3C3F3B)							
Spawning `com.ss.android.ugc.aweme`							
FridaAndroidUtil.curThrowableCls= <class: java.lang.throwable=""></class:>							
<pre>FridaAndroidUtil.JavaArray=<class: java.lang.reflect.array=""></class:></pre>							
FridaAndroidUtil.JavaArrays= <class: java.util.arrays=""></class:>							
FridaAndroidUtil.JavaArrayList= <class: java.util.arraylist=""></class:>							
FridaAndroidUtil.JavaObjAnn_sclass: [b>							
INTEnvIdy CallObjectMathod=34							
lava is available							
Java.androidVersion=13							
Spawned `com.ss.android.ugc.aweme`. Resuming main thread!							
[M2101K9C::com.ss.android.ugc.aweme]-> libName=libsscronet.so							
libraryName=libsscronet.so, callback_afterLibLoaded=function afterLibLoaded=function afterLibLoaded=fu	ded_libsscronet(li	.braryName) {					
<pre>console.log("libraryName=" + libraryName)</pre>							
hookNative_SSL_CTX()							
}							
android_dlopen_ext=0x/d4616a0b8							
Begin Hook							
libraryName=libsscronet so							
oriaEuncPtr verifv=0x79d2692fb0							
func_verify=0x79d2692fb0							
newFuncPtr_verify=0x7d4616e0b8							_
SSL_CTX_set_custom_verify calling: ctx=0x7b8c2b2f78, mode=1, callback=0x	79d13ce5b8						
<pre>SSL_CTX_set_custom_verify calling: ctx=0x7b8c2e5bf8, mode=1, callback=0x</pre>	78ecb1d038						
<pre>SSL_CTX_set_custom_verify calling: ctx=0x7b8c30b718, mode=1, callback=0x</pre>	78ecb1d038						
<pre>SSL_CTX_set_custom_verify calling: ctx=0x7b8c307ed8, mode=1, callback=0x</pre>	78ecb1d038						
SSL_CIX_set_custom_verify calling: ctx=0x7b8c2fe8d8, mode=1, callback=0x	78ecb1d038						
SSL_CIX_set_custom_verity_calling: ctx=0x7b8c507258, mode=1, callback=0x	78ecD10038						
SI_CTX_set_custom_verify_calling: ctx=0x7b6c521656, mode=1, callback=0x	78ecb1d038						
SSL CTX set custom verify calling: ctx=0x7b8c3036f8, mode=1, callback=0x	78ecb1d038						
SSL_CTX_set_custom_verify calling: ctx=0x7b8c2ceb38, mode=1, callback=0x	78ecb1d038						
FridaAndroidUtil.curThrowableCls= <class: java.lang.throwable=""></class:>							
FridaAndroidUtil.JavaArray= <class: java.lang.reflect.array=""></class:>							
FridaAndroidUtil.JavaArrays= <class: java.util.arrays=""></class:>							
<pre>FridaAndroidUtil.JavaArrayList=<class: java.util.arraylist=""></class:></pre>							
FridaAndroidUtil.JavaByteArr= <class: [b=""></class:>							
FridaAndroidUtil.JavaObjArr= <class: [ljava.lang.object;=""></class:>							
JNIENVIAX.CallobjectMethod=34							
Java andraidVersion-13							

效果:

抖音可以正常访问网络了:



crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-06-02 11:44:27

修改并替换libsscronet.so库文件的方式

此处,要去给抖音的 libsscronet.so 去patch打补丁 == 修改并替换 libsscronet.so 的so库文件的方 式:

实现绕过证书校验,实现反反抓包的效果:

修改libsscronet.so的so库文件

要patch的点=具体位置:

先是从函数 SSL_CTX_set_custom_verify 的调用的地方:

通过IDA,可以找到函数 SSL_CTX_set_custom_verify 的实际二进制内偏移地址是: 0x52EF30



通过:

SSL_CTX_set_custom_verify == 0x52EF30

找到2处引用:

.plt:00000000052EF30 .plt:0000000052EF30 .plt:0000000052EF30 .plt:00000000052EF30 .plt:00000000052EF30 .plt:00000000052EF34 .plt:00000000052EF33 .plt:00000000052EF33	set_custom_verify ; CODE XREF: sub_378DF4	.+8C†p
Direction Typ Address	xrefs to SSL_CTX_set_custom_verify Text	
Image: Up p sub_378DF4+8C Image: Up p sub_49BC2C+28	BL SSL_CTX_set_custom_verify BL SSL_CTX_set_custom_verify	
Line 1 of 2	Help Search Cancel OK	

->

- sub_378DF4 + 8C
 - .text:000000000378E7C MOV W1, #1
- sub_49BC2C + 28
 - .text:00000000049BC48 MOV W1, #1

加上 opcode 后显示为:

- sub_378DF4
 - .text:000000000378E7C 21 00 80 52 MOV W1, #1

	🛅 Сору	^ C	i64 (libsscronet.so) /Us	ers/crifan/dev/dev_	root/androidRev	erse			/libsscronet	/staticAna	lysis/ID	A/libsscron	et.so.i64
👩 🖬 i <table-cell></table-cell>	Begin selection Select all	ΥL	🕨 🗛 🖾 🔾	oð 🖻 🕈 📌 -	* 🖬 🗙		No debug	jger	0		2	1 🕈 Ҟ	
1	Select identifier			1									- E
-	Undo General	¥7											
Library functio	Pada	A 9P 7	struction Data	Unexplored Ext	ernal symbol 📃	Lumina f	unction						
Functions		1. 90 L	IDA View-A	× 🖸 Hex	View-1	× 🖪	Structures	× 🖽	Enums	×	* =	Imports	×
	Export data	ΦE	.text:0000	000000378E6C 2B D	3 06 94		BL	SSL_CTX_set	_reverify_or	_resume			
nction name			.text:0000	000000378E70 80 0	2 40 F9		LDR	X0, [X20]					
imp_SSL_CTX	🚮 Code	С	.text:0000	000000378E78 02 B	A FF 10		ADR	X2, sub 378	588				
imp_SSL_aler	d Data	D	• .text:0000	000000378E7C 21 00	80 52		MOV	W1, #1					
imp_SSL_set1	At Struct yor	37.0	.text:0000	000000378E80 2C D	3 06 94		BL	SSL_CTX_set	_custom_ver:	ify			
imp_SSL_CTX	A Struct val	C Q	.text:0000	000000378E84 80 0	2 40 F9		LDR	X0, [X20]					
imp_SSL_get_	'S [™] Strings	>	• .text:0000	000000378E8C 2E D	3 06 94		BL	SSL CTX set	session car	the mode			
<pre>imp_SSL_set_</pre>	📌 Array	*	.text:0000	000000378E90 80 0	2 40 F9		LDR	X0, [X20]					
<pre>imp_SSL_set_</pre>	X Undefine	U	.text:0000	000000378E94 1F 20	0 03 D5		NOP						
imp_SSL_get_	- Ponama	N	.text:0000	000000378E98 81 1	2 00 10		ADR	X1, SUD_3/9	0E8 s set new ch				
imp_SSL_earl	Rename	14	.text:0000	000000378EA0 80 0	2 40 F9		LDR	X0. [X20]	s_sec_new_cr	,			
imp_SSL_proc	Operand type	>	.text:0000	000000378EA4 01 C	2 81 52		MOV	W1, #0×E10					
imp_SSL_rese	operana type		.text:0000	000000378EA8 34 D	3 06 94		BL	SSL_CTX_set	_timeout				
imp_SSL_prov	Comments	,	.text:0000	000000378EAC 80 0.	2 40 19		LDR	X0, [X20] W1 #1					
imp_SSL_is_s	Segments	>	.text:0000	000000378EB4 37 D	3 06 94		BL	SSL CTX set	grease enab	oled			
imp_ERR_prin	Structs	>	.text:0000	000000378EB8 95 0	2 40 F9		LDR	X21, [X20]					
imp_SSL_quic	Functions	>	.text:0000	000000378EBC 85 4/	A FE 97		BL	sub_30B8D0					
<pre>imp_SSL_get_</pre>	Datah ara aram		Change buts		3 00 AA 3 15 AA		MOV	X0, X21					
<pre>imp_EVP_get_</pre>	Patch program	,	Change byte	8 D8	3 06 94		BL	SSL_CTX_set	0_buffer_poo	01			
imp_SSL_CIPI	Other	>	Change word	0 03	2 40 F9		LDR	X0, [X20]	-				
imp_SSL_CIPI	Plugins	>	Assemble	F 20	0 03 D5		NOP	¥1 aub 270	269				
imp_pow		_	Patched bytes	ATP AD	3 06 94		BL	SSL CTX set	msg callbag	k			
imp_log			Apply potobas to input i	0.00	2 40 F9		LDR	X0, [X20]					
imp_exp2			Apply patches to input	ile 5 9/	A 00 94		BL	sub_39F874					
			.text:0000	000000378FF4 F0 0	3 13 AA		MOV	X0. X19					

- sub_49BC2C
 - .text:000000000049BC48 21 00 80 52 MOV W1, #1

IDA - libsscronet.so.i64 (libsscronet.so) /Users/cr	ifan/dev/dev_root/android	Reverse		soLibs/libsscr	onet/staticAn	alysis/ID/	A/libsscrone	et.so.i64
ት 🐴 🐁 🐥 🖡		i 🖻 🛷 🖈 🖬 🗡	(:	No debugger		۵ الا	2	P 🕅	
		l l							
legular function 📕 Instruc	tion 📃 Data 📕 Unexp	lored External symbol	Lumina function	on					
🛛 🗛 🗛 🖂 🚺	IDA View-A	🛛 🖸 Hex View-1	× 🖪 Stri	uctures ×	Enums	×	1	Imports	×
000	.text:000000000	49BC38 FD 03 00 91	MOV	X29,	, SP				
	.text:000000000	49BC3C F3 03 00 2A	MOV	W19,	WØ				
c_method	.text:000000000	49BC40 06 01 00 94	BL	sub_	_49C058 #off_54E428@PAG	F			
tring_long	.text:000000000	49BC48 21 00 80 52	MOV	W1,	#1				
_list	.text:000000000	49BC4C F4 03 00 AA	MOV	X20,	, X0				
sion_psk_dhe_1	.text:000000000	49BC50 42 14 42 F9	LDR	X2,	[X2,#off_54E428	@PAGE0FF]			
x			Patch Bytes			чегіту			
e_legacy_codep	•								
nsport_params	Address	0x49BC48				_on_resume			
ic_transport_pa	F ¹ (()	0.400040							
ccepted	 File offset 	0x49BC48				cache mode			
c_post_handsha	 Original value 	21 00 80 52 F4 03 00 AA	42 14 42 F9 B7 4C	02 94					
data_reject									
_data	Values	01 00 80 52 F4 03 00 A	4 42 14 42 F9 B7 4	C 02 94		ch			
	•								
_fp									
andshake_flight_		Help	Cancel	K		ta_enabled			
ata_reason	•					<101			
ynid	.text:000000000	49BC94 FD 7B C2 A8	LDP	X29,	X30, [SP+var s	0],#0x20			
_prf_nid	.text:000000000	49BC98 BF 23 03 D5	AUT	IASP	-				

根据之前的hook思路,就是:

让传递给 SSL_CTX_set_custom_verify 的参数中 mode 参数的值从 1 改为 0 , 而 mode 参数值, 是保 存在 w1 中的, 所以就是去:

把 w1 的值(从之前的 1)改为 0

分别去改为:

- sub_378DF4
 - .text:000000000378E7C 01 00 80 52 MOV W1, #0

1		1						5	
Library function Regular function	Instruction	Data Unexplored	External symbol	al 📕 Lumina function					
Functions		View-A × 🖪 Pseud	locode-A ×	Hex View-1 ×	\Lambda Structures 🛛 🔀 Enums	× 🛐	Imports) × 🛃	Exports
		.text:0000000000378E08	00 02 80 52	MOV	W0, #0x10 ; size				
unction name		.text:00000000003/8E0C	8E 4D FD 97	BL	SUD_200444				
<pre>fimp_SSL_CTX_set_quic_method</pre>	•	.text:0000000000378E14	F3 03 00 AA	MOV	X19. X0				
fimp_SSL_alert_desc_string_long	•	.text:000000000378E18	9F 8E 00 F8	STR	XZR, [X20,#8]!				
imp_SSL_set1_sigalgs_list		.text:000000000378E1C	F1 D4 06 94	BL	CRYPT0_library_init				
<u>imp_SSL_CTX_set_session_psk_dhe_1</u>		.text:0000000000378E20	E0 03 1F AA	MOV	X0, XZR				
fimp_SSL_get_SSL_CTX		text:00000000000378E24	E1 03 1F AA	MOV	¥2 ¥78				
imp_SSL_set_quic_use_legacy_codep	•	.text:0000000000378E2C	E3 03 1F AA	MOV	X3. XZR				
fimp_SSL_set_quic_transport_params	•	.text:000000000378E30	E4 03 1F AA	MOV	X4, XZR				
<pre>Fimp_SSL_get_peer_quic_transport_pa</pre>	:	.text:000000000378E34	21 D8 06 94	BL	SSL_get_ex_new_index				
7 imp SSL early data accepted		.text:000000000378E38	60 02 00 B9	STR	W0, [X19]				
imp SSL process quic post handsha		.text:000000000378E3C	28 08 06 94	BL	SSL CTY new				
imp_SSL_process_quic_post_itatiustia		text:000000000378E40	F1 03 00 AA	MOV	X1. X0				
imp_SSL_reset_early_data_reject	•	.text:0000000000378E48	E0 03 14 AA	MOV	X0. X20				
/imp_ssl_provide_quic_data		.text:000000000378E4C	2C 00 00 94	BL	sub_378EFC				
fimp_SSL_is_server		.text:000000000378E50	80 02 40 F9	LDR	X0, [X20]				
<pre>imp_ERR_print_errors_fp</pre>		.text:0000000000378E54	1F 20 03 D5	NOP	Ma				
fimp_SSL_quic_max_handshake_flight_		.text:00000000003/8E58	01 00 00 10 52 02 15 AA	ADR	X1, SUD_3/8F18				
imp_SSL_get_early_data_reason		.text:0000000000378E60	28 08 06 94	BI	SSL CTX set cert ch				
fimp_EVP_get_digestbynid	•	.text:000000000378E64	80 02 40 F9	LDR	X0. [X20]				
<pre>//imp_SSL_CIPHER_get_prf_nid</pre>		.text:000000000378E68	21 00 80 52	MOV	W1, #1				
imp SSL CIPHER get id		.text:000000000378E6C	2B D8 06 94	BL	SSL_CTX_set_reverify_on_resume				
imp pow		.text:000000000378E70	80 02 40 F9	LDR	X0, [X20]				
imp log		.text:000000000378E74	02 BA FF 10	ADB	X2. sub 378588				
imp_ovp2	•	.text:0000000000378E7C	01 00 80 52	MOV	W1. #0				
/mp_cxpz	•	.text:000000000378E80	2C D8 06 94	BL	SSL_CTX_set_custom_verify				
imp_memcpy	•	.text:000000000378E84	80 02 40 F9	LDR	X0, [X20]				
fimpstack_chk_fail		.text:000000000378E88	21 60 80 52	MOV	W1, #0x301				
fimp_memmove		.text:000000000378E8C	21 08 06 94	BL	SSL_LIX_SET_SESSION_Cache_mode				
fimp_malloc_usable_size		.text:000000000378E90	1F 20 03 D5	NOP	AU, [A20]				
fimp_memset	•	.text:000000000378E98	81 12 00 10	ADR	X1. sub 3790E8				
jimp_android_fdsan_exchange_owner_	•	.text:000000000378E9C	31 D8 06 94	BL	SSL_CTX_sess_set_new_cb				
f imp_getifaddrs		.text:000000000378EA0	80 02 40 F9	LDR	X0, [X20]				
7 imp freeifaddrs		.text:000000000378EA4	01 C2 81 52	MOV	W1, #0×E10				
		.text:00000000003/8EA8	34 D8 06 94 80 02 40 F9	BL	SSL_CIX_Set_Timeout				
ine 20932 of 20932		00378F7C 00000000000378F	7C: sub 378DE	4+88 (Synchronized wit	h Hex View-1)				
Output									
stopper using gacasea cypeincov sub_		·							
39FA28: using guessed typeint64fa	stcall sub_3	9FA28(_QWORD, _QWORD);	0001						
SAI040: USING guessed typeint64ia	stcall Sub_3	alease records (OWORD, _QWORD, _QW	OWORD OWORD						
52ED20: using guessed typeint64i	stcall SSL g	et0 signed cert timestamp	list(OWORD.	OWORD, OWORD):					
52ED98: using guessed typeint64fa	stcall SSL_g	et0_peer_certificates(_QW	(ORD);						
3785B8: using guessed typeint64 var_	30;								
Python									
.,									

- sub_49BC2C
 - .text:00000000049BC48 01 00 80 52 MOV W1, #0

	IDA - libsscronet	t.so.i64 (libss	cronet.so) /	Users/crifan/dev	/dev_root	/androidRe	verse	oL	ibs/libsscron	et/staticAnaly	sis/IDA/libs	scronet.so.i	64		
8 🛃 8 🖨 🗧 🖨 🗸	n n n a	• 🖡 🖪	. 🔺 🥥	े 📩 💣 🕷	st- 🖈	🖬 🗙	No debug	iger		😊 🐮 🖻	i 🗊 🕈	*			
						1							b		0
Library function	Regular function	Instruction	Data	Linexplored	External	symbol	Lumina function								
7 Functions			View-A	× 🖪 Pseud	locode-A	× 🖸	Hex View-1 × A	Structures	× 🖽	Enums	× 🕅	Imports	× 🛃	Exports	-
			text:00	0000000049BC2C	3F 23 03	D5	PACIASP	-							
Function name			.text:00	00000000049BC30	FD 7B BE	A9 A9	STP	X29, X30, X20 X19	[SP,#-0x20+	var_s0]!					
<pre>imp_SSL_CTX_set_iimp_SSL_CTX_set_iimp_SSL_CTX_set_iimp_SSL_CTX_set_iimp_SSL_CTX_set_iimp_SSL_CTX_set_iimp_SSL_CTX_set_iimp_SSL_CTX_set_iimp_SSL_CTX_set_iimp_SSL_CTX_set_iimp_SSL_CTX_set_iimp_SSL_CTX_set_iimp_SSL_CTX_set_iimp_SSL_CTX_set_iimp_SSL_SEt_i _</pre>	quic_method	•	.text:00	00000000049BC38	FD 03 00	91	MOV	X29, SP	tor for the lost						
imp_SSL_alert_desc	_string_iong		.text:00	0000000049BC3C	F3 03 00	2A	MOV	W19, W0							
/imp_SSL_set1_sigar	gs_list		.text:00	00000000049BC40	00 01 00	94	BL	SUD_49C050	5						
<pre>imp_SSL_CTX_set_</pre>	session_psk_ane_i	•	.text:00	00000000049BC48	01 00 80	52	MOV	W1. #0	J4L420@FAGL						
/imp_sst_get_sst_t			.text:00	0000000049BC4C	F4 03 00	AA	MOV	X20, X0							
Fimp_SSL_set_quic_i	use_legacy_codep		.text:00	0000000049BC50	42 14 42	F9	LDR	X2, [X2,#0	off_54E428@P	AGEOFF]					
imp_SSL_set_quic_i	transport_params		.text:00	00000000049BC54	E0 03 14	AA	MOV	35L_UIX_S6 X0, X20	et_custom_ve	TTTY					
<pre>imp_SSL_get_peer_</pre>	quic_transport_pa	•	.text:00	00000000049BC5C	21 00 80	52	MOV	W1, #1							
imp_SSL_early_data	_accepted	:	.text:00	0000000049BC60	AE 4C 02	94	BL	SSL_CTX_se	et_reverify_	on_resume					
imp_SSL_process_c	uic_post_handsha		.text:00	0000000049BC64	E0 03 14	AA	MOV	X0, X20							
fimp_SSL_reset_earl	y_data_reject		text:00	00000000049BC66	B7 4C 02	94	BI	SSI CTX S	et session c	ache mode					
imp_SSL_provide_q	uic_data	•	.text:00	0000000049BC70	1F 20 03	D5	NOP	550_011_51	cc_session_e	dene_mode					
fimp_SSL_is_server			.text:00	0000000049BC74	61 01 00	10	ADR	X1, sub_49	9BCA0						
imp_ERR_print_erro	rs_fp		.text:00	00000000049BC78	EØ Ø3 14	AA	MOV	X0, X20		-					
imp_SSL_quic_max_	_handshake_flight_	•	.text:00	00000000049BC7C	61 02 00	12	AND	W1, W19, 4	ess_set_new_	co					
imp_SSL_get_early_	data_reason	•	.text:00	0000000049BC84	E0 03 14	AA	MOV	X0, X20							
fimp_EVP_get_diges	tbynid		.text:00	0000000049BC88	FE 4C 02	94	BL	SSL_CTX_se	et_early_dat	a_enabled					
imp_SSL_CIPHER_g	et_prf_nid		.text:00	00000000049BC8C	E0 03 14	AA	MOV	X0, X20	[CD #ups of	01					
imp_SSL_CIPHER_g	et_id		.text:00	00000000049BC90	FD 7B C2	A9 A8	LDP	X20, X19, X29, X30,	[SP+var_s1	.#0x20					
🗲imp_pow		•	.text:00	00000000049BC98	BF 23 03	D5	AUTIASP	ALS, ASU,	[51 1401_30]	,					
📝imp_log		•	.text:00	0000000049BC9C	C0 03 5F	D6	RET								
fimp_exp2			.text:00	0000000049BC9C		; } //	starts at 49BC2C								
imp_memcpy			.text:00	000000000498090		; End	of function sub_49BC2C								
F _ imp _ stack chk fa	ail		.text:00	00000000049BCA0											
imp memmove			.text:00	0000000049BCA0		;	S U B R O U	T I N E ====							
imp malloc usable	e size		.text:00	0000000049BCA0											
imp memset			.text:00	00000000049BCA0		; Attr	ibutes: bp-based frame	tpd=0x20							
imp android fdsan	exchange owner		.text:00	00000000049BCA0		sub 49	BCAR		DATA XREE:	sub 498C2C+4	810				
imp getifaddrs	exenange_enner_		.text:00	00000000049BCA0		0002.0									
imp_getildddrs			.text:00	0000000049BCA0		var_20	= -0×20								
			.text:00	00000000049BCA0		var_10	= -0×10								
Line 20932 of 20932			0049BC48	00000000000049BCA0	248: sub_	49BC2C+1C	(Synchronized with He	ex View-1)							
Output															
- output		370000(10107													
39FA28: using guessed 3A1840: using guessed	typeint64fa	stcall sub_3	9FA28(_QWO A1840(_QWO	RD, _QWORD); RD. OWORD. OW	(ORD):										
52ED08: using guessed	typeint64fa	stcall SSL_g	et0_ocsp_r	esponse(_QWORD,	_QWORD,	_QWORD);									
52ED20: using guessed	typeint64fa	stcall SSL_g	et0_signed_	_cert_timestamp	_list(_QW	(ORD, _QWOF	RD, _QWORD);								
378588: using guessed	typeint64fa	sicali SSL_gi 30:	er@_peer_ce	ercificates(_QW	iunD);										
stosses, using guessed	cybeincod val_														
Python															
U: idle Down	Disk: 54GB														

替换libsscronet.so的so库文件

本身手动即可去替换修改后的so库文件,到安卓手机中已安装的app的相关路径下面的旧的so库文件

不过为了简化,目前已写成搅脚本自动化操作:

/Users/crifan/dev/dev_root/androidReverse/xxx/Douyin/dy297/Douyin/dy297/libsscronet_so/aut oReplaceSo/autoReplaceSo.sh

```
#!/bin/bash
# Function: Script to auto replace Douyin libsscronet.so
# Author: Crifan Li
# Update: 20240923
# SEPERATOR="-----"
SEPERATOR="================="
function log() {
  echo "${SEPERATOR} $1 ${SEPERATOR}"
}
LIBSSCRONET_SO="libsscronet.so"
echo "LIBSSCRONET_SO=${LIBSSCRONET_SO}"
SO_NEW_PATH_PC="/Users/crifan/dev/dev_root/androidReverse/xxx/Douyin/dy297/Douyin/dy297
/libsscronet_so/input/libsscronet_yyy.so"
# S0_NEW_PATH_PC="/Users/crifan/dev/dev_root/androidReverse/xxx/Douyin/dy297/Douyin/dy2
97/libsscronet_so/input/libsscronet_crifan.so"
# SO_NEW_PATH_PC="/Users/crifan/dev/dev_root/androidReverse/xxx/Douyin/dy313/input/libs
scronet/libsscronet_yyy.so"
echo "SO_NEW_PATH_PC=${SO_NEW_PATH_PC}"
SO_TEMP_DOWNLOAD_FOLDER="/sdcard/Download/"
echo "S0_TEMP_DOWNLOAD_FOLDER=${S0_TEMP_DOWNLOAD_FOLDER}"
```

```
S0_TEMP_DOWNLOAD_PATH="${S0_TEMP_DOWNLOAD_FOLDER}/${LIBSSCRONET_S0}"
 echo "S0_TEMP_DOWNLOAD_PATH=${S0_TEMP_DOWNLOAD_PATH}"
 # echo "${SEPERATOR} Download ${LIBSSCRONET_SO} into android ${SEPERATOR}"
 log "Download ${LIBSSCRONET_SO} into android"
 adb push ${SO_NEW_PATH_PC} ${SO_TEMP_DOWNLOAD_FOLDER}/${LIBSSCRONET_SO}
 # echo "${SEPERATOR} Find ${LIBSSCRONET_SO} location ${SEPERATOR}"
 log "Find ${LIBSSCRONET_SO} location"
 # LIBSSCRONET_SO_ROOT_FOLDER="/data/app"
 LIBSSCRONET_SO_ROOT_FOLDER="/data/data" # /data/data/com.ss.android.ugc.aweme/app_libra
 rian/29.7.0.6746496378/libsscronet.so
 SO_FILE_ANDROID=$(adb shell find ${LIBSSCRONET_SO_ROOT_FOLDER} -name ${LIBSSCRONET_SO})
 echo "S0_FILE_ANDROID=${S0_FILE_ANDROID}"
 # echo "${SEPERATOR} Extract ${LIBSSCRONET_SO} folder path ${SEPERATOR}"
 log "Extract ${LIBSSCRONET_SO} folder path"
 # S0_FOLDER_ANDROID=${S0_FILE_ANDROID#libsscronet}
 # S0_FOLDER_ANDROID=${S0_FILE_ANDROID##libsscronet}
 # SO_FOLDER_ANDROID=${${SO_FILE_ANDROID}#libsscronet.so}
 SO_PATH_LEN=${#SO_FILE_ANDROID}
 echo "S0_PATH_LEN=${S0_PATH_LEN}"
 SO_FILE_LEN=${#LIBSSCRONET_SO}
 echo "SO_FILE_LEN=${SO_FILE_LEN}"
 S0_F0FER_LEN=$((${S0_PATH_LEN}-${S0_FILE_LEN}))
 echo "SO_FOFER_LEN=${SO_FOFER_LEN}"
 # S0_FOLDER_ANDROID=${S0_FILE_ANDROID##libsscronet}
 # S0_FOLDER_ANDROID=${S0_FILE_ANDROID%libsscronet}
 # SO_FOLDER_ANDROID=${SO_FILE_ANDROID:96}
 # SO_FOLDER_ANDROID=${SO_FILE_ANDROID:0:97}
 S0_FOLDER_ANDROID=${S0_FILE_ANDROID:0:${S0_FOFER_LEN}}
 echo "S0_FOLDER_ANDROID=${S0_FOLDER_ANDROID}"
 # echo "${SEPERATOR} Into adb shell ${SEPERATOR}"
 log "Into adb shell"
 adb shell <<EOF
 uname -a
 ls -lh ${SO_TEMP_DOWNLOAD_FOLDER} | grep ${LIBSSCRONET_SO}
 # cd /data/app
 # pwd
 # find . -name libsscronet.so
 # SO_FILE_ANDROID=$(find , -name libsscronet.so)
 # echo "S0_FILE_ANDROID=${S0_FILE_ANDROID}"
 cd ${SO_FOLDER_ANDROID}
 # echo "${SEPERATOR} Into ${SO_FOLDER_ANDROID} ${SEPERATOR}"
 log "Into ${SO_FOLDER_ANDROID}"
 # echo "${SEPERATOR} Remove ${LIBSSCRONET_SO} ${SEPERATOR}"
 log "Remove ${LIBSSCRONET_SO}"
 ls -lh | grep ${LIBSSCRONET_SO}
 rm -f ${LIBSSCRONET_SO}
 ls -lh | grep ${LIBSSCRONET_SO}
 # echo "${SEPERATOR} Move ${LIBSSCRONET_SO} to here ${SEPERATOR}"
 log "Move ${LIBSSCRONET_SO} to here"
 mv ${S0_TEMP_DOWNLOAD_PATH} ${S0_FOLDER_ANDROID}
```

```
ls -lh | grep ${LIBSSCRONET_SO}
# echo "${SEPERATOR} Change permission for ${LIBSSCRONET_SO} ${SEPERATOR}"
log "Change permission for ${LIBSSCRONET_SO}"
chmod 755 ${LIBSSCRONET_SO}
chown system ${LIBSSCRONET_SO}
chgrp system ${LIBSSCRONET_SO}
ls -lh | grep ${LIBSSCRONET_SO}
EOF
```

之前某次的运行效果:

```
→ libsscronet_so autoReplaceSo/autoReplaceSo.sh
 LIBSSCRONET_SO=libsscronet.so
 SO_NEW_PATH_PC-/Users/crifan/dev/dev_root/androidReverse/xxx/DouYin/dy297/libsscronet_s
 o/input/libsscronet_crifan.so
 SO_TEMP_DOWNLOAD_FOLDER=/sdcard/Download/
 SO_TEMP_DOWNLOAD_PATH=/sdcard/Download//libsscronet.so
                      Download libsscronet.so into android
 /Users/crifan/dev/dev_root/androidReverse/xxx/...: 1 file pushed, 0 skipped. 97.4 MB/s (
 5567544 bytes in 0.055s)
                      Find libsscronet.so location
 SO_FILE_ANDROID=/data/app/~~cJq-AFnKyZwZZqpRJY9hWA ==/com.ss.android.ugc.aweme-1LCghzY2H
 KvNbI0WF3vccQ //lib/arm64/libsscronet.so
                      Extract libsscronet.so folder path
 SO PATH LEN=111
 SO_FILE_LEN=14
 SO_FOFER_LEN=97
 S0_F0LDER_ANDROID=/data/app/~~cJq-AFnKyZwZZqpRJY9hWA=/com.ss.android.ugc.aweme-1LCghzY
 2HKvNbI0WF3vccQ /lib/arm64/
                      Into adb shell
 Linux localhost 4.19.269 #1 SMP PREEMPT Sat Jul 27 21:05:42 CST 2024 aarch64 Toybox
 -rw-rw---- 1 u0_a216 media_rw 5.3M 2024-08-28 09:41 libsscronet.so
 /data/app/~~cJq-AFnKyZwZZqpRJY9hWA /com.ss.android.ugc.aweme-1LCghzY2HKvNbI0WF3vccQ /
 lib/arm64
 -rwxr-xr-x 1 system system 5.3M 2024-04-22 22:06 libsscronet.so
 -rw-rw---- 1 u0_a216 media_rw 5.3M 2024-08-28 09:41 libsscronet.so
 -rwxr-xr-x 1 system system 5.3M 2024-08-28 09:41 libsscronet.so
4
                                                                                        F
```

替换so后,重启抖音,抖音即可正常访问网络:

Android版



正常抓包了。

附录

如何确定要修改的值的逻辑 = 应该修改二进制指令为何值?

此处是要修改函数 SSL_CTX_set_custom_verify 的参数,此处是第二个参数= mode 参数=存放在 W1 中的值:从 1 变成 0

MOV W1, #1 改为: MOV W1, #0 如何把要改的指令生成对应的Opcode操作码? 而已知要去把: MOV W1, #0 的改动写入到so库文件中,但是对应的opcode操作码的值是什么,此时并不知道 所以可以借助于 指令和二进制opcode互转 · 最流行汇编语言: ARM 中的: Online ARM to HEX Converter (armconverter.com) 去生成此处的,ARM64的二级制的汇编指令码 从而才能搞懂: 原始的字节码 -》 对应的汇编代码含义 以及,要修改成什么汇编代码-》所对应的新的字节码是多少 举例: 之前的汇编代码是: MOV W1, #1 对应着:

21008052

ARM64的字节码是:

而要改为:

MOV

对应的ARM64字节码是:

01008052

》所以我们最终要改的数据就是:

W1, #0

- 从: 21 00 80 52
- 改为: 01 00 80 52

-》对应到IDA中就是

- 0x378E7C
 - Origin value
 - 21 00 80 52 2C D8 06 94 80 02 40 F9 21 60 80 52
 - 注: 后续有更多的二进制字节码,不用管,保持原始值即可
 - 2C D8 06 94 80 02 40 F9 21 60 80 52
 - 且后续注意到: 是后续其他3行汇编代码对应的汇编指令

.text:000000000378E80	2C	D8	06	94	BL	SSL_CTX_set_
custom_verify						
.text:000000000378E84	80	02	40	F9	LDR	X0, X20
.text:000000000378E88	21	60	80	52	MOV	W1, #0×301

- Values
 - 01 00 80 52 2C D8 06 94 80 02 40 F9 21 60 80 52

IDA - libsscronet.so.i64 (libsscronet.so) /Users/c	rifan/dev/dev_root/androidReverse		oLibs/libsscro	onet/staticAnalysis/	IDA/libsscronet.	so.i64
h 🐴 🐁 🐥 🖡 🗛 i 🛛 🤤 i 🚮	🗄 💣 🛷 裙 🖬 🗙 🕬	🔲 🔲 No debug	ger	 1 1	1 🕈 🏌	
						1 1 (
egular function 📕 Instruction 📗 Data 📕 Unexp	olored 📒 External symbol 📒 Lum	ina function				
n n n 🔉 🛛 🖪 IDA View-A	< 🖸 Hex View-1 🛛 🛛 🗚	Structures	× 🛅 Enums	× 🛐	Imports	× 🖻
.text:00000000	0378E6C 2B D8 06 94 0378E70 80 02 40 F9	BL LDR	<pre>SSL_CTX_set_reverif X0, [X20]</pre>	y_on_resume		
ic_method .text:00000000	0378E78 02 BA FF 10	ADR	X2, sub 3785B8			
string_long .text:00000000	0378E7C 21 00 80 52	MOV	W1, #1			
_list .text:00000000	0378E80 2C D8 06 94	BL	SSL_CTX_set_custom_	verify		
ssion_psk_dhe_1	03/8684 80 02 40 F9	LDR	X0, [X20]			
	Patch B	ytes		ache_mode		
e_legacy_codepi						
ic transport pa	0x378E7C					
rccepted · File offset	0x378E7C			cb		
c post handsha	21 00 80 52 20 08 06 04 80 02	40 50 21 60 90 52				
data reject	2100 80 52 20 08 00 94 80 02	40 F9 21 00 80 52				
data Values	01 00 80 52 2C D8 06 94 80 02	40 F9 21 60 80 52				
				abled		
fp •				JUCCU		
andshake_flight_	Help Cance					
ata_reason						
/nid .text:00000000	0378EC8 38 D8 06 94	BL	SSL_CTX_set0_buffer	_pool		

IDA中如何修改二进制=打补丁=patch

- 概述
 - 。 IDA->Edit-》Patch program-》Change byte-》修改数据-》OK
 - IDA->Edit- Patch program- Apply patches to input file- OK
- 详解

• 打补丁·逆向利器: IDA

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-06-03 09:43:01

iOS版抖音

绕过iOS版抖音的证书绑定校验

比如iOS版 抖音 内部就做了证书校验

想要逆向,绕过抖音的证书绑定校验话,可以通过写hook代码绕过证书校验,即可实现抓包 HTTPS 看到明 文数据。

具体步骤:

之前已给此处iPhone7搭建过Charles抓包环境:

- 已安装过Charles的根证书: charles-ssl-proxying-certificate.cer
 - 。 且已信任过

此处只需要去:

把Charles的SSL根证书放入iPhone中对应的的位置,比如:

/Library/PreferenceLoader/Preferences/charles/charles-ssl-proxying-certificate.cer

然后再去写hook代码:

// to fix Charles capture https show Unknown issue
// https://bbs.pediy.com/thread-270700.htm
// https://iosre.com/t/topic/20202/46

```
#define CHARLES_CERT_FILE @"/Library/PreferenceLoader/Preferences/charles/charles-ssl-p
roxying-certificate.cer"
```

bool cfgHookEnable_aweme = true;

```
hook TTNetworkManagerChromium
  (NSArray )ServerCertificate {
    iosLogDebug("%s", "");
   NSArray' serverCertList = %orig();
   iosLogDebug("serverCertList=%{public}@", serverCertList);
    1111
           NSString *serverCertListStr = [NSArray nsStrListToStr:serverCertList isSort
List:FALSE isAddIndexPrefix:TRUE];
     NSString *serverCertListStr = [CrifanLibHookiOS nsStrListToStr:serverCertList isS
11
ortList:FALSE isAddIndexPrefix:TRUE];
11
     iosLogInfo("serverCertListStr=%{public}@", serverCertListStr);
11
//// return nil;
11
    return serverCertList;
```

```
NSMutableArray newCertList = [NSMutableArray arrayWithArray serverCertList];
    iosLogDebug("newCertList=%{public}@, newCertList.count=%{public}lu", newCertList, [
newCertList count]);
    if (cfgHookEnable_aweme) {
        NSString certResourcePath = CHARLES_CERT_FILE;
        iosLogDebug("certResourcePath=%{public}@", certResourcePath);
        NSFileManager defaultManager = [NSFileManager defaultManager];
        BOOL isExistedCert = [defaultManager fileExistsAtPath: certResourcePath];
        iosLogInfo("isExistedCert=%s", boolToStr(isExistedCert));
        if (isExistedCert) {
           NSData certP12Data = [NSData dataWithContentsOfFile: certResourcePath];
            iosLogDebug("certP12Data=%{public}@", certP12Data);
            [newCertList addObject: certP12Data];
            iosLogDebug("newCertList=%{public}@, newCertList.count=%{public}u", newCer
tList, [newCertList count]);
        3
    }
   NSMutableArray retNewCertList = [newCertList copy];
   iosLogDebug("retNewCertList=%{public}@", retNewCertList);
   return retNewCertList;
 end
```

再去Charles做好基本的代理配置:

- Charles中开启代理
- iPhone中使用Mac中的Charles代理

即可顺利实现iPhone7中抖音的https的抓包,看到https的明文了:

				Charles	s 4.6.3b2 - Session 1 *					
			> •		• 🤊 C 🗸	> ©				
structure	Seque	nce								
Code	Method	Host	Path				Start D	uration	Size Status	
200	CONNECT	api5-normal-c-lq.amemv.com					14:41:52		18.08 KBFailed	
200	CONNECT	api5-normal-c-lq.amemv.com					14:41:52		18.20 KBFailed	
200	CONNECT	api5-normal-c-lq.amemv.com					14:41:52		18.08 KBFailed	
200	CONNECT	api5-normal-c-lq.amemv.com					14:41:52		18.08 KBFailed	
200	CONNECT	api5-normal-c-lq.amemv.com					14:41:52		18.20 KBFailed	
200	CONNECT	api5-normal-c-lq.amemv.com					14:41:52		18.08 KBFailed	
200	CONNECT	api5-normal-c-lq.amemv.com					14:41:52	7.85 s	18.62 KBComple	te
200	POST	log3-misc-lq.amemv.com	/service/2/	device_register/?dev	rice_id=3843&is_activat	ted=0&aid=1128&tt_data=a&	14:41:53	278 ms	22.82 KBComple	te
200	POST	log3-misc-lq.amemv.com	/service/2/	log_settings/?packag	e=com.ss.iphone.ugc.Aweme&appThem	e=light&version_code=18.9	14:41:53	289 ms	169.67 KBComple	te
200	POST	log3-misc-lq.amemv.com	/service/2/	app_log/?package=c	om.ss.iphone.ugc.Aweme&appTheme=li	ght&version_code=18.9.0&n	14:41:53	146 ms	4.78 KBComple	te
200	POST	security-lq.snssdk.com	/api/byte/c	onfig/v5/?et=0&coun	try=CN&uvc=189034&app_name=com.	ss.iphone.ugc.Aweme&chan	14:41:53	223 ms	21.22 KBComple	te
200	GET	api5-core-c-la.amemv.com	/aweme/v2	/feed/?package=com	n.ss.iphone.uac.Aweme&appTheme=liaht	&need personal recommen	14:41:53	1.82 s	70.59 KBComple	te
r:									Focused	Setting
thod: Po hority: I eme: ht h: /ice/2/d	OST og3-misc-l tps evice_regis	q.amemv.com iter/?device_id=33&is	activated=0&aid=1128	&tt_data=a&packag	ge=com.ss.iphone.ugc.Aweme&appTh	eme=light&version_code=18	.9.0&need_	personal_	recommend=1&js_	sdk_ver
thod: P0 hority: I neme: ht h: vice/2/d tent-len 1128	OST og3-misc-l tps evice_regis gth: 1094	q.amemv.com tter/?device_id=33&is_a	activated=0&aid=1128	&tt_data=a&packaç	ge=com.ss.iphone.ugc.Aweme&appTh	eme=light&version_code=18	.9.0&need_	personal_	recommend=1&js_	sdk_ver
thod: P(hority: I neme: ht h: vice/2/d tent-len 1128 s-cookie	OST og3-misc-l tps evice_regis gth: 1094 : install_id	q.amemv.com tter/?device_id=3 3&is_s =2 9; ttreq=1\$d675 = 5 000 10 000 000 000 000 000 000 000 00	activated=0&aid=1128	&tt_data=a&packag	ge=com.ss.iphone.ugc.Aweme&appTh	eme=light&version_code=18	.9.0&need_ 708	personal_	recommend=1&js_	sdk_ver
thod: P0 hority: I neme: ht h: vice/2/d tent-len 1128 s-cookie _tt=3	DST og3-misc-l tps evice_regis gth: 1094 : install_id	q.amemv.com iter/?device_id=38is_ =2	activated=0&aid=1128	&tt_data=a&packag 16f; d 1cc; passport	ge=com.ss.iphone.ugc.Aweme&appTh ticket=f26 _csrf_token=7	neme=light&version_code=18	.9.0&need_ 708 srf_token_d	personal_ lefault=72	recommend=1&js_	sdk_ver
thod: P0 hority: I eme: ht h: vice/2/d tent-len 1128 -cookie tt=3 -version tent-typ	DST og3-misc-l tps evice_regis gth: 1094 : install_id: : 2 e: applicat	q.amemv.com :ter/?device_id=3 3&is_: =2: 9; ttreq=1\$d675 -c; uid_tt_ss=371*** ion/octet-stream;tt-data=a	activated=0&aid=1128	&tt_data=a&packag 16f; d îcc; passport	ge=com.ss.iphone.ugc.Aweme&appTh 1_ticket=f28 _csrf_token=7	neme=light&version_code=18 control introls; multi_sids= db; passport_co	.9.0&need_ 708 srf_token_d	personal_ lefault=72	recommend=1&js_	sdk_ver
thod: P(hority: I eme: ht h: vice/2/d tent-len 1128 s-cookie tt=3 -version tent-typ -token:	DST og3-misc-l tps evice_regis gth: 1094 : install_id : 2 e: applicat 00b5ef7	q.amemv.com :ter/?device_id=3 3&is_s =2 9; ttreq=1\$d675 c; uid_tt_ss=371 ion/octet-stream;tt-data=a	activated=0&aid=1128	&tt_data=a&packag 16f; d 	ge=com.ss.iphone.ugc.Aweme&appTh 1_ticket=f2f0occocc _csrf_token=7	eme=light&version_code=18 b; multi_sids= db; passport_ct	.9.0&need_ 708 srf_token_d	personal_ lefault=72	recommend=1&js_)2dd8f675d	sdk_ver
thod: PC hority: I eme: ht h: vice/2/d tent-len 1128 -cookie tt=3 -version tent-typ -token: -acent	DST og3-misc-l tps evice_regis gth: 1094 : install_idi : 2 e: applicat 00b5ef7 Awene 18	q.amemv.com ter/?device_id=3 3&is_t =2 9; ttreq=1\$d675 .c; uid_tt_ss=371 ion/octet-stream;tt-data=a 9.0 pr:199034 /ibbnae: inc 13.3.1: sb. C String Cockes Test Hav	activated=0&aid=1128	&tt_data=a&packag 16f; c "cc; passport	ge=com.ss.iphone.ugc.Aweme&appTf J_ticket=f20 _csrf_token=7	eeme=light&version_code=18 	.9.0&need_ 708 srf_token_d	personal_ lefault=72	recommend=1&js_)2dd8f675d	sdk_ver 07f8019
thod: PC hority: I here: ht h: vice/2/d tent-len 1128 s-cookie _tt=3 -version tent-typ -token: r-acent: leaders	DST og3-misc-l tps evice_regis gth: 1094 : install_id : 2 e: applicat 00b5ef7 Awgene 18 Query S	q.amemv.com :ter/?device_id=3 3&is_: =2: 9; ttreq=1\$d67٤ -c; uid_tt_s=371 ion/octet-stream;tt-data=a 9.0.pc:189034./jDbone: iOS 13.2.1: zh. C String Cookies Text Hex	activated=0&aid=1128	&tt_data=a&packag 16f; d ,cc; passport	ge=com.ss.iphone.ugc.Aweme&appTh 1_ticket=f28 _csrf_token=7	eme=light&version_code=18	.9.0&need_ 708 srf_token_d	personal_ lefault=72	recommend=1&js_)2dd8f675d	sdk_ver: 07f8019
thod: PC hority: I here: ht h: vice/2/d tent-len 1128 s-cookie tt=3 -version tent-typ -token: r-acent: leaders	DST pg3-misc-l tps evice_regis gth: 1094 : install_id: : 2 e: applicat 00b5ef7 Awame 18 Query 5	q.amemv.com tter/?device_id=3 3&is_t =2 9; ttreq=1\$d675 oc; uid_tt_ss=371 ion/octet-stream;tt-data=a 9.0 nr/189034 /iPhone: iOS 13 3 1 - 25 0 String Cookies Text Hex =2 9; ttreq=1\$d75 0 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 -	activated=0&aid=1128	&tt_data=a&packag 16f; c	ge=com.ss.iphone.ugc.Aweme&appTh i_ticket=f20ocrf_token=7	eme=light&version_code=18	.9.0&need_ 708 srf_token_d	personal_ lefault=72	recommend=1&js_)2dd8f675d	sdk_ver
thod: PC hority: I neme: ht h: vice/2/d tent-len 1128 s-cookie tt=3 -version tent-typ -token: r-acent: eaders	DST pg3-misc-l tps evice_regis gth: 1094 : install_id : e: applicat 00b5ef7 Aweme 18 Query 5 id_str": ", 0,	q.amemv.com iter/?device_id=3 3&is_r =2 9; ttreq=1\$d675 =>c; uid_tt_ss=371*** ion/octet-stream;tt-data=a 9.0 nv:180024.ijbhone: iOC 13.2 1->h C String Cookies Text Hex **2 19**,	activated=0&aid=1128	8tt_data=a&packag 16f; g Tec; passport	ge=com.ss.iphone.ugc.Aweme&appTf 1_ticket=f28 _csrf_token=7	eme=light&version_code=18	.9.0&need_ 708 srf_token_d	personal_ lefault=72	recommend=1&js_)2dd8f675d	sdk_ver 07f8019
thod: PC hority: I heme: ht h: vice/2/d tent-len 1128 s-cookie tt=3 -version tent-typ -token: r-acent: eaders install hew_use	SST gg3-misc-l tps evice_regis gth: 1094 : instal_id : astal_id : astal	q.amemv.com :ter/?device_id=3 3&is_i =2: 9; ttreq=1\$d67{ :c; uid_tt_ss=371** ion/octet-stream;tt-data=a 9.0.pc:189034 //Dhone: iOS 13.2.1: 2h C String Cookies Text Hex *2 19", MASE(activated=0&aid=1128 NI Cropet Raw	16f; d 16f; d 1cc; passport	ge=com.ss.iphone.ugc.Aweme&appTh 1_ticket=f28 _csrf_token=7	eme=light&version_code=18	.9.0&need_ 708 srf_token_d	personal_ lefault=72	recommend=1&js_)2dd8f675d 41",	sdk_ver 07f8019
thod: PC hority: I teme: ht h: vice/2/d tent-len 1128 s-cookie tt=3 -version tent-typ -token: -acent eaders install new_use device_ server_	SST gg3-misc-l tps evice_regis gth: 1094 : install_id : 2 e: applicat O0b5cf7 Awema 18 Query 5 : ": 0, token": "A time": 165 d": 3	q.amemv.com iter/?device_id=3 3&is_i =2 9; ttreq=1\$d675 	activated=0&aid=1128	8tt_data=a&packag 116f; d icc; passport	ge=com.ss.iphone.ugc.Aweme&appTh i_ticket=f20ionionoon _csrf_token=7	eme=light&version_code=18 	.9.0&need_i 708 srf_token_d	personal_ lefault=72	recommend=1&js_)2dd8f675d 41",	sdk_ver 07f8019
thod: PC thority: I teme: ht th: vice/2/d tent-len 1128 s-cookie _tt=3 tent-typ -token: r-acent leaders install new_use device_ install	SST og3-misc-l tps evice_regis gth: 1094 : install_id : e: applicat 00b5ef7 Awema 18 Query S id_str": "": 0, time": 165 id": 2	q.amemv.com tter/?device_id=3 3&is_r =2 9; ttreq=1\$d675 =>c; uid_tt_ss=371 ion/octet-stream;tt-data=a 9.0 nv:190024./jbhone: iOC 13.2 1-b C String Cookies Text Hex **? 19", AASE 39, 19", 39, 19", 39, 19", 39, 19", 39, 19", 39, 19", 39, 19", 39, 19", 39, 19, 19", 39, 19, 19", 39, 19, 19", 39, 19, 19", 39, 19, 19, 19, 19, 19, 19, 19, 19, 19, 1	activated=0&aid=1128	8tt_data=a&packag 16f; 3cc; passport	ge=com.ss.iphone.ugc.Aweme&appTh 1_ticket=f2f0osrf_token=7	eme=light&version_code=18	.9.0&need_1 708 srf_token_d	personal_ lefault=72	recommend=1&js_)2dd8f675d 41°°,	sdk_ver
thod: P0 thority: I heme: ht th: vice/2/d tent-len 1128 s-cookie _tt=31 -version tent-typ -roken: -roken: -token: install new_use device_ install device_	SST og3-misc-l tps evice_regis gth: 1094 : install_id : install_id : applicat OOb5ef7 Awama 18 Query 5 id_str": " : 0, time": 165 id": 2 id_str": "	q.amemv.com iter/?device_id=3 3&is_i =2: 9; ttreq=1\$d675 :c; uid_tt_ss=371 ion/octet-stream;tt-data=a 9.0.0c:189034 (iPbone: iOS 13.3.1: zh. C string Cookies Text Hex "2 19", MASE 3892913, 39, 31, 31, 31, 31, 31, 31, 31, 31	activated=0&aid=1128	16f; d 16f; d 1cc; passport	ge=com.ss.iphone.ugc.Aweme&appTh 1_ticket=f280 _csrf_token=7	eme=light&version_code=18	.9.0&need_1 708 srf_token_d	personal_ lefault=72	recommend=1&js_)2dd8f675d 41''',	sdk_ver
thod: PC hority: I teeme: ht h: vice/2/d tent-len 1128 s-cookie tt=3 -version tent-typ -token: -acenti- eaders install device_ install device_	SST og3-misc-l tps evice_regis gth: 1094 : install_id : ce: applicat OOD567/ Awama 18 Query: : "": 0, : token": "/ token": "/ token": "/ token": "/	q.amemv.com iter/?device_id=3 3&isi =2 9; ttreq=1\$d675 -c; uid_tt_ss=371 ion/octet-stream;tt-data=a 9.0.pr:190324 (ibbone: iOC 13.2.1: zb. C string Cookles Text Hex "2 19", AASEC 3892913, 34, 35, 35, 36, 37, 37, 37, 37, 38, 38, 38, 38, 38, 38, 38, 38	activated=0&aid=1128	8tt_data=a&packag 116f; d icc; passport	ge=com.ss.iphone.ugc.Aweme&appTh j_ticket=f2e	eme=light&version_code=18	.9.0&need_ 708 srf_token_d	personal_ lefault=72	recommend=1&js_)2dd8f675d 4I**,	sdk_ver
thod: PC hority: I heme: ht h: vice/2/d tent-len 1128 s-cookie _tt=3 -version tent-typ -token: r-acent: leaders install new_use device_ device_	<pre>DST opg3-misc-l tps evice_regis gth: 1094 : install_id </pre>	q.amemv.com tter/?device_id=3 3&is_r =2 9; ttreq=1\$d675 =>c; uid_tt_ss=371 ion/octet-stream;tt-data=a 9.0 nv:190024.ijbnne: iOC 13 2 1 - b C String Cookies Text Hex *2 19", AASE 3892913, 3, 39, 39, 39, 39, 39, 39, 39, 39, 39, 39,	activated=0&aid=1128	8tt_data=a&packag 116f; d "Cc; passport	ge=com.ss.iphone.ugc.Aweme&appTh i_ticket=f280ocrf_token=7	eme=light&version_code=18	.9.0&need_ 708 srf_token_d	personal_ lefault=72	recommend=1&js_)2dd8f675d 41°°,	sdk_ver
thod: PC hority: I h: vice/2/d tent-len 1128 s-cookie tt=3 -version tent-typ -version tent-typ -version tent-typ -version tent-typ -version seaders server_use fevice_ server_ server serv	SST bgg3-misc-l bgs evice_regis gth: 1094 : install_id : 2 : 2 : 4 : e: applicat OObSef7 Auroma 18 Query 5 id_str": " : 0; : 10; : 10; : 2 : 2 : 2 : 2 : 2 : 2 : 2 : 2	q.amemv.com tter/?device_id=3 3&is_r =2 9; ttreq=1\$d675 =0; vid_tt_ss=371*** ion/octet-stream;tt-data=a 9.0 nv:190024.ijBhone: iOC 13.2.1** h String Cookies Text Hex ************************************	activated=0&aid=1128	&tt_data=a&packag 16f; d "cc; passport "cc; passport	ge=com.ss.iphone.ugc.Aweme&appTh i_ticket=f20	eme=light&version_code=18	.9.0&need_ 708 srf_token_d	personal_ lefault=72	recommend=1&js_)2dd8f675d 4I**,	sdk_ver

- 注:此处代码只对当时的某些版本,比如:抖音 17.8 、18.9 ,是有效的
 - 。-》目前最新版本抖音,此代码已无效。
 - -》 但是也有人说,最新版本也是有效的。待各位自己确认核实。

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-06-02 10:39:55

附录

下面列出相关参考资料。

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-05-30 17:31:49

参考资料

- 【已解决】绕过抖音反抓包网络错误: Frida去hook校验函数SSL_CTX_set_custom_verify
- 【已解决】绕过抖音反抓包网络错误:给libsscronet.so二进制打补丁patch
- 【记录】IDA中给libsscronet.so打补丁patch program修改二进制
- 【记录】给抖音douyin297.apk替换库文件libsscronet.so
- 【记录】给改机小米的Pixel5中的抖音: 替换库文件libsscronet.so
- 【已解决】安卓adb push导入文件报错: adb error failed to copy remote couldn't create file Permission denied
- 【已解决】安卓手机中寻找已安装抖音的data数据的目录
- 【已解决】mitmdump抓包改机小米后的Pixel5中抖音失败且抖音提示:网络错误,当前无网络,请检查后重试
- 【已解决】用脚本自动化处理替换apk中so库文件libsscronet.so的过程
- 【记录】抖音so库libsscronet.so:静态分析
- 【记录】给抖音v29.7.0去替换libsscronet.so库
- 【记录】给抖音31.3.0的apk替换libsscronet.so使得可以访问网络和抓包
- 【记录】抖音的反抓包相关网络错误: libsscronet.so库和SSL_CTX_set_custom_verify
- 【记录】对比libsscronet.so二进制打补丁的区别:别人修改的和我们修改的
- 【记录】研究疑似libmetasec_ml.so调用到libsscronet.so函数: Cronet_Engine_SetOpaque
- •
- SSL证书绑定 · iOS安全与防护 (crifan.org)
- tiktok加密参数分析_tiktik iid-CSDN博客
- android逆向奇技淫巧二十九: x音AES使用分析 第七子007 博客园
- Disable SSL pinning using Frida (github.com)
- •

crifan.org, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新: 2025-06-03 09:43:15