目录

iOS越狱开发：常用越狱插件

- 最新版本：`v1.0.0`
- 更新时间：`20240711`

简介

介绍iOS逆向期间，iPhone越狱相关的，常用的一些插件。以及iOS越狱后初始化逆向开发环境概述；

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/ios_re_common_tweak: iOS越狱开发：常用越狱插件

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

- iOS越狱开发：常用越狱插件 book.crifan.org
- iOS越狱开发：常用越狱插件 crifan.github.io

离线下载阅读

- iOS越狱开发：常用越狱插件 PDF
- iOS越狱开发：常用越狱插件 ePub
- iOS越狱开发：常用越狱插件 Mobi

版权和用途说明

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

越狱插件概述

- 常用越狱插件概述
  - `OpenSSH`：通过ssh访问iPhone
  - `Filza`：最常用的、最好用的文件管理器
  - `AFC2 = Apple File Conuit "2"`：允许通过USB访问iPhone
    - 由此支持相关工具：`iFunBox` 、 `3uTools` 、 `爱思助手`
  - `AppSync Unified`：让系统不再验证签名
    - app安装就不会，因为签名原因而安装失败了
  - `CocoaTop64`：查看进程详情
    - 比如：进程的Flag、二进制文件位置等等
  - `iCleaner Pro`：插件管理
    - 比如：临时开启或禁用某个/某些插件
  - `Mterminal`：iPhone内的终端工具
  - `绕过ssl certificate pinning`：绕过SSL certificate pinning=SSL证书绑定的一些相关插件
    - 概述
      - 最好用的是：`NyaMisty/ssl-kill-switch3`
      - 其次是：`evilpenguin/SSLBypass`
      - 再次是
        - `nabla-c0d3/ssl-kill-switch2`
        - `julioverne` 的 `SSL Kill Switch 2 (iOS 13)`

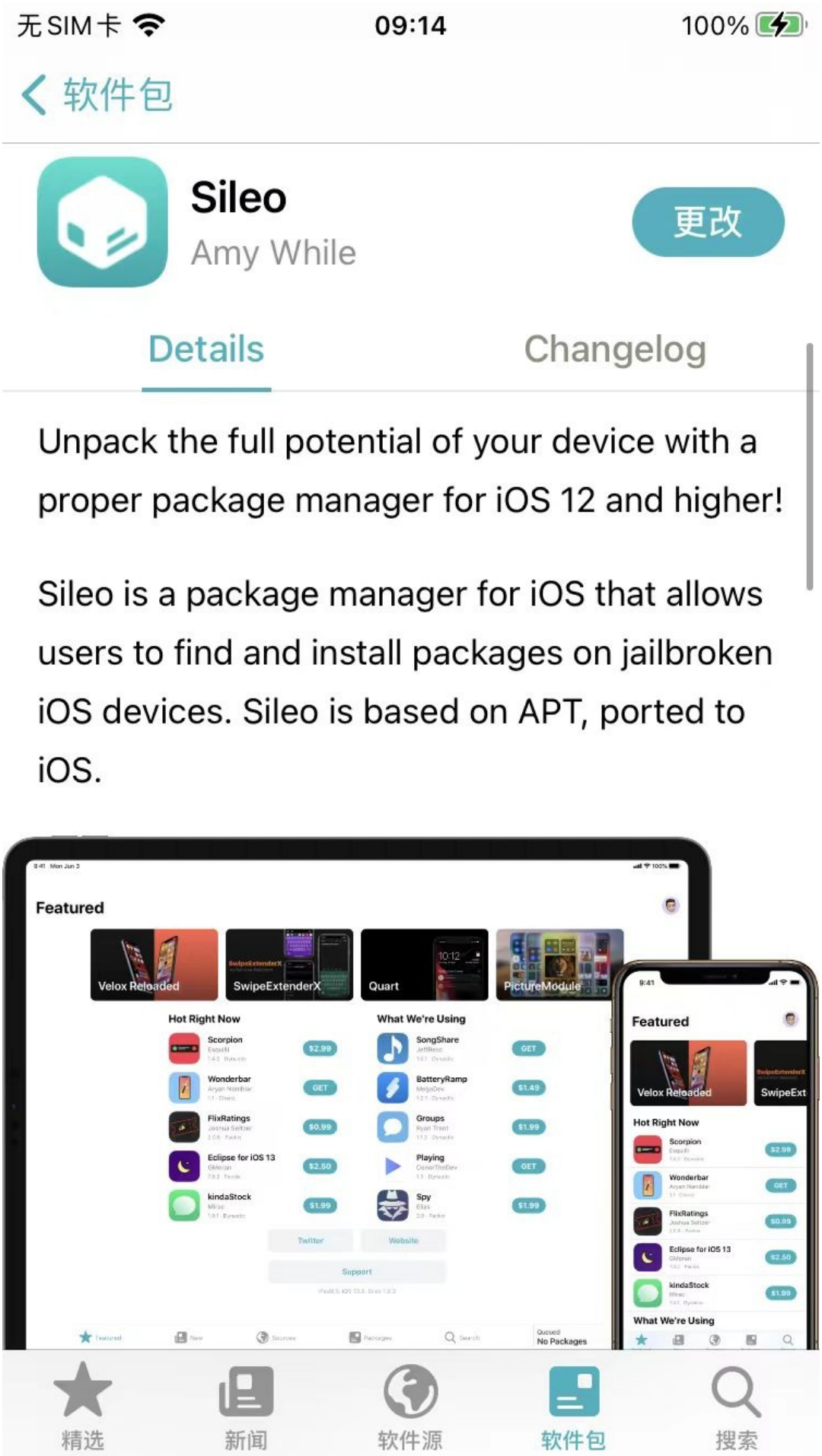
下面详细介绍具体插件的功能和用法。

初始化逆向开发环境

此处整理和介绍，iOS越狱后，初始化逆向开发环境，常常需要做的事情 = 逆向开发环境初始化 的相关内容

其中主要也就是一些常用插件的安装和设置：

- 包管理器
  - Sileo
    - 源地址：https://repo.getsileo.app
    - 安装后


无SIM卡
09:14
100%
软件包
Sileo
Amy While
更改
Details
Changelog
Unpack the full potential of your device with a proper package manager for iOS 12 and higher!
Sileo is a package manager for iOS that allows users to find and install packages on jailbroken iOS devices. Sileo is based on APT, ported to iOS.
Featured
Velox Reloaded
SwipeExtenderX
Quart
PictureModule
Hot Right Now
What We're Using
Scorpion
Wonderbar
FlixRatings
Eclipse for iOS 13
kindaStock
SongShare
BatteryRamp
Groups
Playing
Spy
Twitter
Website
Support
No Packages
精选
新闻
软件源
软件包
搜索

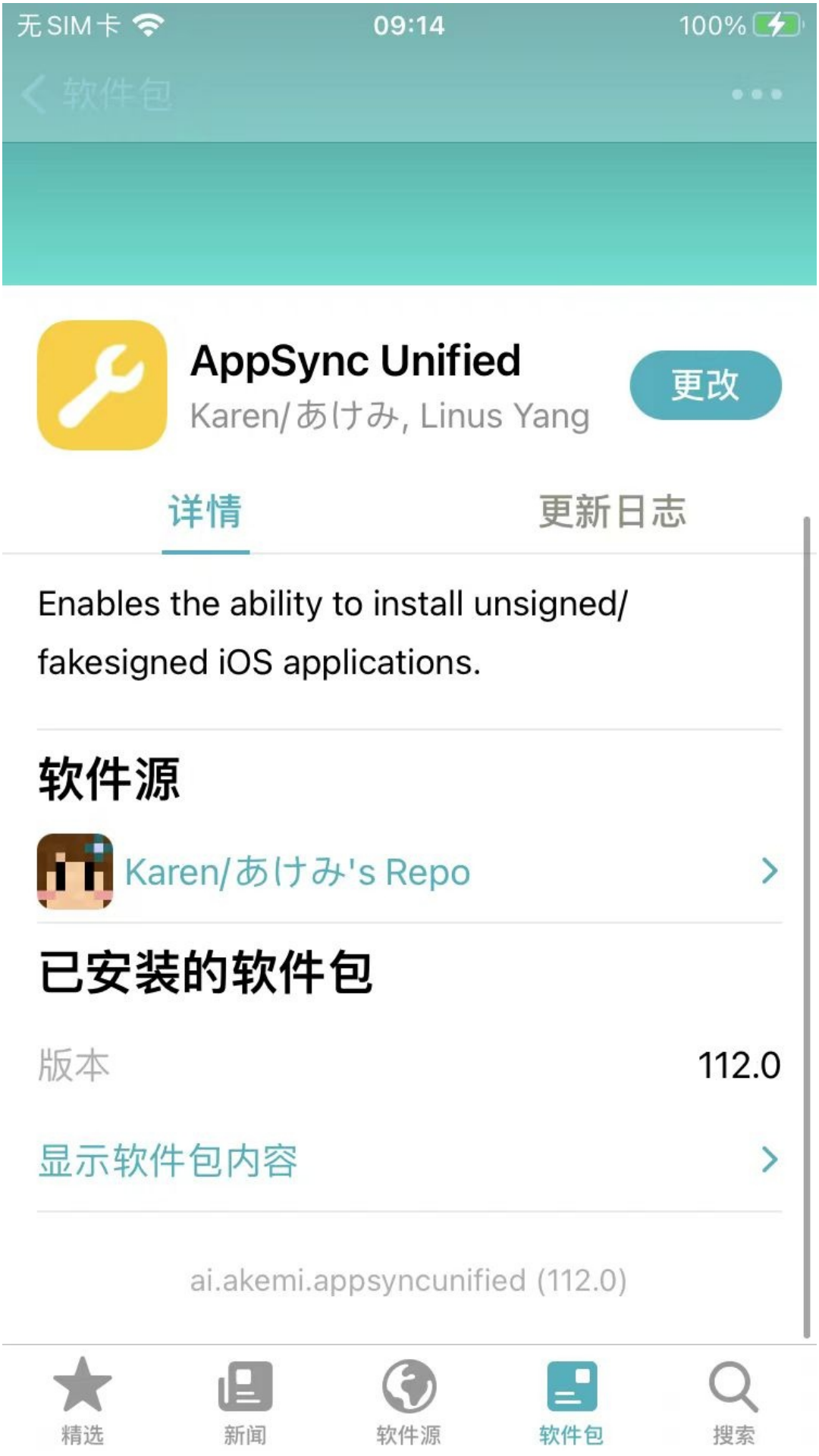
- 文件管理器：
  - Filza
    - 源地址：
      - rootful
        - https://tigisoftware.com/repo/
      - rootless
        - http://apt.thebigboss.org/repofiles/cydia/
    - 安装后


无SIM卡
09:14
100%
软件包
Filza File Manager
TIGI Software
更改
详情
更新日志
File Manager for iPhone, iPad, iPod Touch.
Supports iOS 7+
软件源
BigBoss
已安装的软件包
版本
4.0.1-3
显示软件包内容
com.tigisoftware.filza (4.0.1-3)
精选
新闻
软件源
软件包
搜索

- ssh = OpenSSH
  - 源地址
    - https://apt.bingner.com/
  - 安装后
    -


无 SIM 卡
09:15
100%
软件包
OpenSSH
Sam Bingner
更改
详情
更新日志
secure shell (SSH) server, for secure access from remote machines This is the portable version of OpenSSH, a free implementation of the Secure Shell protocol as specified by the IETF secsh working group. . Ssh (Secure Shell) is a program for logging into a remote machine and for executing commands on a remote machine. It provides secure encrypted communications between two untrusted hosts over an insecure network. X11 connections and arbitrary TCP/IP ports can also be forwarded over the secure channel. It can be used to provide applications with a secure communication channel. . This package provides the sshd server. . In some countries it
精选
新闻
软件源
软件包
搜索

    - 相关内容
        - rootful
            - 默认用户：root
                - 默认密码：alpine
            - 用法举例
                - ssh root@192.168.2.24
        - rootless
            - palera1n越狱后
                - 默认用户：mobile
                    - 默认密码：alpine
                - 用法举例：ssh mobile@192.168.2.24
        - 免密登录
            - rootful
                - ssh-copy-id root@192.168.2.24
            - rootless
                - ssh-copy-id mobile@192.168.2.24
- 其他插件
    - AppSync Unified
        - 源地址：https://cydia.akemi.ai/
        - 安装后


无 SIM 卡
09:14
100%
软件包
AppSync Unified
Karen/あけみ, Linus Yang
更改
详情
更新日志
Enables the ability to install unsigned/ fakesigned iOS applications.
软件源
Karen/あけみ's Repo
已安装的软件包
版本
112.0
显示软件包内容
ai.akemi.appsyncunified (112.0)
精选
新闻
软件源
软件包
搜索

- ldid = Link Identity Editor
  - 源地址
    - https://apt.bingner.com/
    - https://apt.procurs.us/
  - 安装后


无SIM卡
09:14
100%
软件包
Link Identity Editor
Jay Freeman (saurik)
更改
详情
更新日志
pseudo-codesign Mach-O files
软件源
Bingner/Elucubratus
已安装的软件包
版本
2:2.1.5-1
显示软件包内容
ldid (2:2.1.5-1)
精选
新闻
软件源
软件包
搜索

        - 作用：给ipa伪签名
            - Filza安装ipa之前，有时候需要用到ldid去伪签名
    - AFC2 = Apple File Conduit "2"
        - 源地址
            - rootful
                - http://apt.thebigboss.org/repofiles/cydia
            - rootless
                - 不支持iOS 15+的rootless
        - 安装后


无SIM卡
09:14
100%
软件包
Apple File Conduit "2" (iOS 11+, arm64)
更改
saurik, Cannathea
详情
更新日志
Allow full file-system access over USB for all arm64 devices, especially useful for those on iOS 11 and above. Please install ldid as it is required for use. (except for the XinaA15 jailbreak)
软件源
BigBoss
已安装的软件包
版本
1.1.8-1
显示软件包内容
com.cannathea.afc2d-arm64 (1.1.8-1)
精选
新闻
软件源
软件包
搜索

Tweak插件来源

其他插件地址，绝大多数都可以在这里找到：

- https://www.ios-repo-updates.com
  - iOS Repo Updates • Cydia iOS Repository Updates for Jailbroken iPhone iPad or iPod (ios-repo-updates.com)

SSH

OpenSSH

TODO：

- 【记录】iPhone中用Cydia安装SSH插件：OpenSSH

文件管理器

Filza

TODO：

- 【记录】已越狱iPhone中使用Filza File Manager
- 【已解决】越狱iOS中用Cydia安装Filza File Manager
- 【记录】越狱iPhone7P中安装Filza
- 【记录】越狱iPhone7P中安装64位的Filza File Manager 64-bit
- 【记录】iPhone7P中用Filza安装抖音ipa

- 安装64位的Filza
  - 概述
    - Cydia源：`http://tigisoftware.com/cydia/` -> `TIGI Software` -> `全部工具` -> `Filza File Manager 64-bit`
  - 详解
    - 【记录】越狱iPhone6P中用Cydia安装Filza File Manager 64-bit

AFC2

TODO：

- 【已解决】已越狱iPhone用Cydia安装Apple File Conuit "2"
- 【已解决】Cydia安装AFC2报错：Can't find a source to download version 1.1.1of apt.zscool.net.arm64:iphoneos-arm

---

- `AFC2` = `Apple File Conuit "2"`

签名

AppSync Unified

TODO：

- 【已解决】已越狱iPhone中用插件AppSync
- 【记录】越狱iPhone7P通过Cydia安装插件：AppSync Unified
- 【已解决】已越狱iPhone中用插件AppSync

- `AppSync` = `AppSync Unified`
  - 用途：让系统不再验证签名-》app安装就不会，因为签名原因而安装失败了

进程

CocoaTop64

- CocoaTop64：查看进程详情
  - 比如查看进程参数 `Raw Process Flags` -》 可以得知进程是否可调试

插件管理

iCleaner Pro

TODO：

- 【已解决】Cydia中如何临时的禁止插件生效而不是只能卸载掉

终端

TODO：

【已解决】越狱iPhone中安装Cydia插件：终端工具

Mterminal

TODO：

- 【已解决】越狱iPhone中用Cydia安装终端工具：Mterminal

NewTerm 2

绕过ssl certificate pinning

TODO：

- SSL Kill Switch 2
  - 【已解决】越狱iPhone中安装越狱插件：SSL Kill Switch 2

- `绕过ssl certificate pinning`：绕过SSL certificate pinning=SSL证书绑定的一些相关插件
  - 概述
    - 最好用的是：`NyaMisty/ssl-kill-switch3`
    - 其次是：`evilpenguin/SSLBypass`
    - 再次是
      - `nabla-c0d3/ssl-kill-switch2`
      - `julioverne` 的 `SSL Kill Switch 2 (iOS 13)`
  - 详见
    - 破解https的SSL Pinning iOS端 · app抓包利器：Charles

附录

下面列出相关参考资料。

参考资料

- Discussion What is AFC2? : r/jailbreak
- iOS Repo Updates • Cydia iOS Repository Updates for Jailbroken iPhone iPad or iPod (ios-repo-updates.com)