

**iOS软件在运行时究竟做了什么：Introspy-iOS**

**译者：tree\_fly(看雪ID：treefly)**

**原文链接：[http://t.cn/RVTonZU](http://t.cn/Rcsj8sN) 原文作者：integrity-sa**

** **

**微信公众号：看雪iOS安全小组 我们的微博：weibo.com/pediyiosteam**

**我们的知乎：zhihu.com/people/pediyiosteam**

**加入我们：看雪iOS安全小组成员募集中：http://bbs.pediy.com/showthread.php?t=212949  
[看雪iOS安全小组]置顶向导集合贴： http://bbs.pediy.com/showthread.php?t=212685**

Blackbox工具可用来协助分析iOS应用程序在运行时做了什么,并挖掘潜在的安全问题。

有关介绍，请查阅： <http://isecpartners.github.io/Introspy-iOS/>

**描述**

安装在越狱设备上的追踪器，可以劫持和记录正在运行应用程序所调用的与安全相关的敏感API。

工具可以记录并存储到数据库的内容包括API调用的详细信息，如参数和返回值等。

此外，也可以实时查看和分析正在监视的API调用信息。

Introspy-Analyzer依据数据库信息，执行一个Python脚本后可创建包含函数调用列表的HTML报告以及潜在的漏洞影响应用程序列表。 Introspy-Analyzer托管在单独的存储库：<https://github.com/iSECPartners/Introspy-Analyzer>

**安装**

请下载最新版本:

<https://github.com/integrity-sa/Introspy-iOS/releases>

早期版本：

<https://github.com/iSECPartners/Introspy-iOS/releases>

**依赖内容**

仅支持越狱设备. 使用Cydia时请确保已安装如下的依赖包：

- dpkg

- Cydia Substrate

- PreferenceLoader

- Applist

**如何安装**

下载并复制安装包到设备中，安装即可:

scp <package.deb> root@<device\_ip>:~

ssh root@<device\_ip>

dpkg -i <package.deb>

重启SpringBoard：

killall -HUP SpringBoard

安装成功后，在设置中有2个菜单，Apps菜单允许你选择对应的程序，Settings菜单可以设置被劫持的API接口。

最后，记得关闭并重新启动被监控的程序。

**如何卸载**

dpkg -r com.isecpartners.introspy

**生成Html报告**

跟踪器会记录程序调用的API相关信息，并存储到数据库中（事实上每个程序都有独立的文件夹）

使用Introspy-Analyzer的脚本，让数据分析变得更加容易，而且可以分析和标记危险的API调用，以方便在iOS应用程序中识别漏洞。

Introspy-Analyzer托管在单独的存储库:

<https://github.com/iSECPartners/Introspy-Analyzer>

**编译 Introspy-iOS**

大部分的使用者只要下载和安装预编译的Debian包即可，如果你想修改功能，自行编译即可。

安装包要求设备安装Theos，参阅 <https://github.com/theos/theos>， 以及Theos的安装文档

<https://github.com/theos/theos/wiki/Installation>.

需要在环境变量中设置 $THEOS , 参考代码：

export THEOS=/absolute/path/to/theos

export PATH=$THEOS/bin:$PATH

编译和生成安装包:

make package

成功编译和生成安装包后，设置好设备的IP地址，随后Theos可以自动将安装包安装到设备中，并重启SpringBoard，代码如下:

export THEOS\_DEVICE\_IP=192.168.1.127

make install

**许可证**

查阅 ./LICENSE.

**作者**

* Tom Daniels
* Alban Diquet

**维护者**

Herman Duarte