# 

**海马iOS应用商店助手各种恶意行为的研究**

**译者：rodster(看雪ID：leixyou)、御宅的鸡蛋℡  
原文链接：http://t.cn/Rcsj8sN原文作者：趋势科技**

** **

**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**

# 海马iOS应用程序商店助手添加恶意行为

**前言**

earlierblog的一篇文章中,我们谈到了iOS海马应用商店。在这里我们发现官方应用程序重新重新打包并且添加了广告模块增加所有者收入。

因为“海马iOS助手”，所以商店很受欢迎的一个原因是它的相对简单的使用性。这个程序是为了补充其他的商店,使它更容易安装应用程序和管理用户的设备。这与大多数iOS用户使用itunes一样。

不幸的是,这个特殊的辅助应用程序自己带来的恶意代码。我们发现这个asTSPY\_LANDMIN.A。

**首先:合法iTunes版本**

这个助手从海马提供下载的网站下载。它提示用户直接从海马下载一个特定版本的iTunes(12.3.2.25)。这个文件是相同的官方versionfrom苹果,虽然不再是iTunes的最新版本。

、

Figure 1. iTunes download prompt

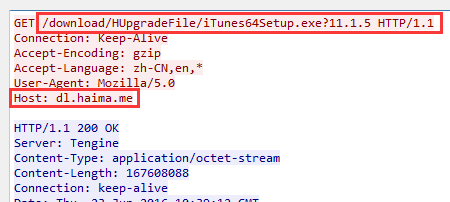


Figure 2. Download from Haima server

一旦iTunes被安装，接下来就会从海马服务器下载一个补丁包。

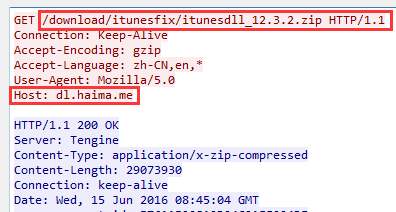


Figure 3. Download of patch package

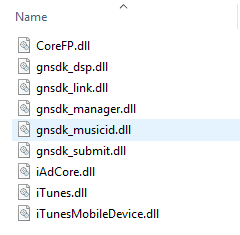


Figure 4. Patch package contents

包中文件被解压到海马目录。

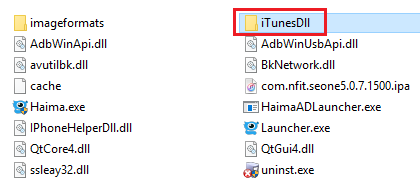


Figure 5. Patch package in Haima directory

补丁中的文件实际上来源于Apple。海马分析基于12.3.2.25版本的iTunes协议，所以海马助手依赖于特定版本的DLL。即使iTunes之后更新了，海马助手仍然可以安装app或者同步备份和从ios设备恢复。

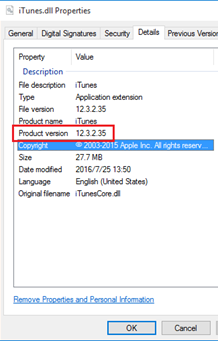


Figure 6. DLL version

**如何安装app**

海马提供了两种方式安装app。在IOS，所有的app被安装都需要被签名，所以海马使用两种方式：一种是使用企业提供证书,而另一种通过 App Store由苹果提供app。下图显示了助手的应用,功能或多或少但也是一个app商店。



Figure 7. Haima helper app

海马助手app有一个应用商店拥有的所有特征——类别,必备列表,建议应用程序,等等。这些应用程序和原来iOS应用程序商店都是一样的,那些已经被我们在上面的截图标记的应用也是。

助手可以用企业证书直接安装应用程序，并且它也能从apple的app store安装应用。我们将稍后在这篇文章中讨论使用企业证书。之后它是怎么做的?它连接回海马服务器和“获得”一个苹果ID:

上面的屏幕显示了海马的用户需要一个苹果ID,并单击按钮,获得一个更好的体验。



上面的窗口状态正在进行验证过程,包括检查的安全环境。



上面的窗口,当一个苹果ID已经成功获取到了。用户甚至不知道这个苹果ID账户的密码,但助手应用程序可以使用这个苹果ID安装任何iOS应用程序到用户的iPhone。

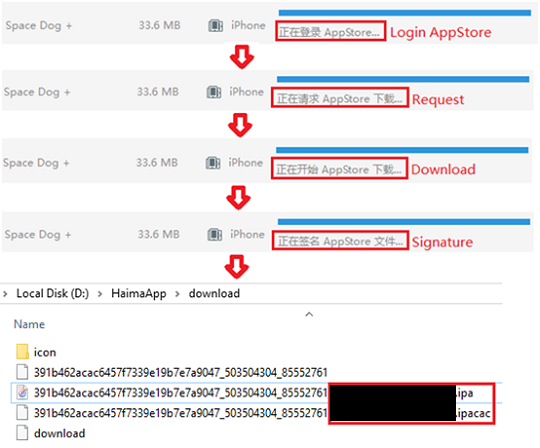


Figure 11. Installation of app with Apple ID

如果用户已经通过app Store安装了一个应用程序,助手会首先要求用户删除这个版本的应用。设备上的助手将更新企业证书,然后(重新)安装手机上的应用程序。



Figure 12. Request to uninstall app

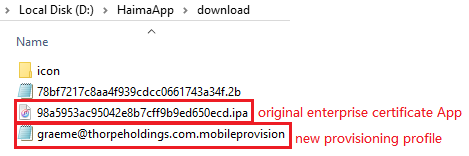
http://blog.trendmicro.com/trendlabs-security-intelligence/files/2016/08/haima13.png

Figure 13. Update for enterprise certificate

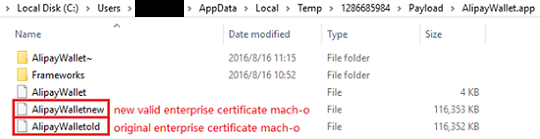
**动态App签名绕过苹果撤销**

如之前所述,助手app还可以使用企业证书安装应用到设备。苹果非常清楚企业如何滥用企业的证书,他们不断地撤销任何此类已被滥用的证书。海马每隔几天替换了他们使用的企业证书。除此之外,他们还使用动态应用的签字来减少暴露企业证书。

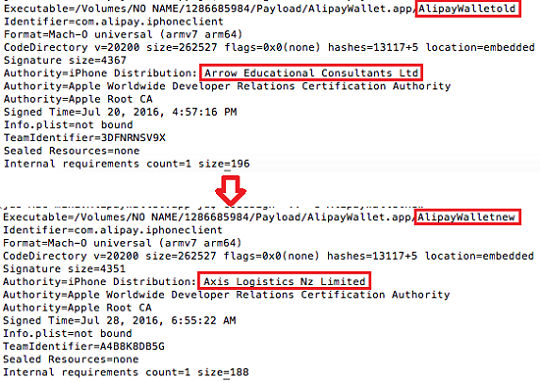
在助手app安装企业证书应用到手机之前,用一个新的企业证书(有效)签字。这是为了防止苹果撤销原企业证书。



*Figure 14. Downloaded Original Enterprise Certificate App and New Provisioning Profile*



*Figure 15. Original and New Enterprise Certificate Mach-O Files*



*Figure 16. From Original Certificate to New*

**用户Apple ID泄露**

还有第三种方法来安装应用程序。如果你不想使用Haima-provided苹果ID,您可以使用你的——你只需要输入自己的苹果ID和密码。



Figure 17. Login screen asking for Apple ID

不幸的是,这不是一个好主意。为什么?因为助手app窃取用户的用户名和密码。

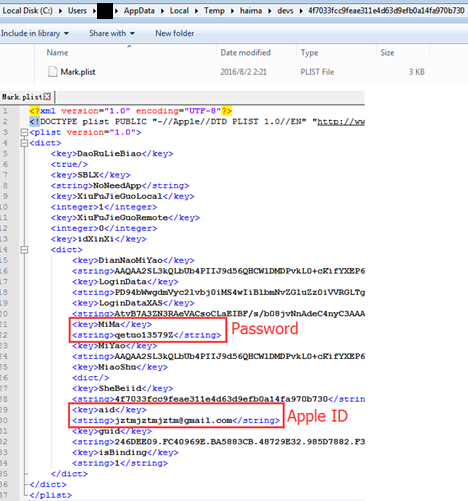


Figure 18. Code leaking Apple ID

**照片同步到PC**

默认情况下,这些照片在iPhone上不同步到电脑。然而,助手app自动同步用户的照片到用户的计算机：

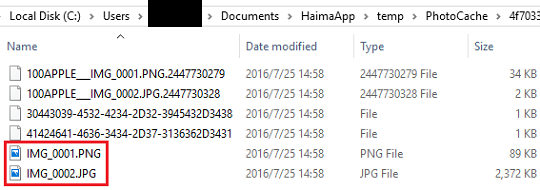


Figure 19. Synced pictures

**助手App中的恶意代码**

因为各种information-stealing helper函数调用，海马助手app包含恶意代码。然而,这些既非功能性需要或也非必须被调用。

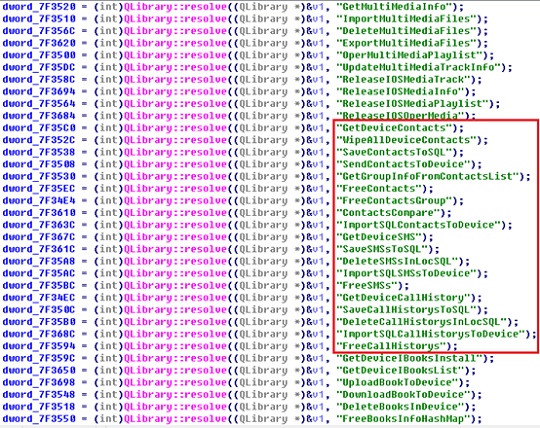


Figure 20. Malicious code

**总结**

海马助手app是让第三方为它的用户存储更有用的一个关键部分。通过管理企业证书和苹果应用商店登录,让用户更加无缝体验。

然而,它也引入了严重的安全风险。明显的窃取用户的苹果ID凭证本身是一个严重的风险。明显的恶意功能代码本身也是令人担忧的。我们不建议使用第三方应用商店一般构成安全风险,这种情况下显示了为什么我们建议了这篇文章。

我们发现以下文件并命名为TSPY\_LANDMIN.A:

|  |  |
| --- | --- |
| ***SHA1哈希*** | ***文件名称*** |
| 1 fd7073ffd23e6b57be7418be24b78cd3694fe2f | IPhoneHelperDll.dll |
| 8 d13df388e1dae9d0100967190d4d4b32bd25b8f | 00 \_4.3.7.exe |
| ec58ec2ecc019d5c927acfa7520550c35d1b480c | Haima.exe |