Monthly Research

The diffusion of malware by malicious development environment

FFRI,Inc.
http://www.ffri.jp

Ver 1.00.01

Agenda

- Introduction
- About XcodeGhost
- A case in Android
- Concerns of new attack
- Countermeasures
- Summary

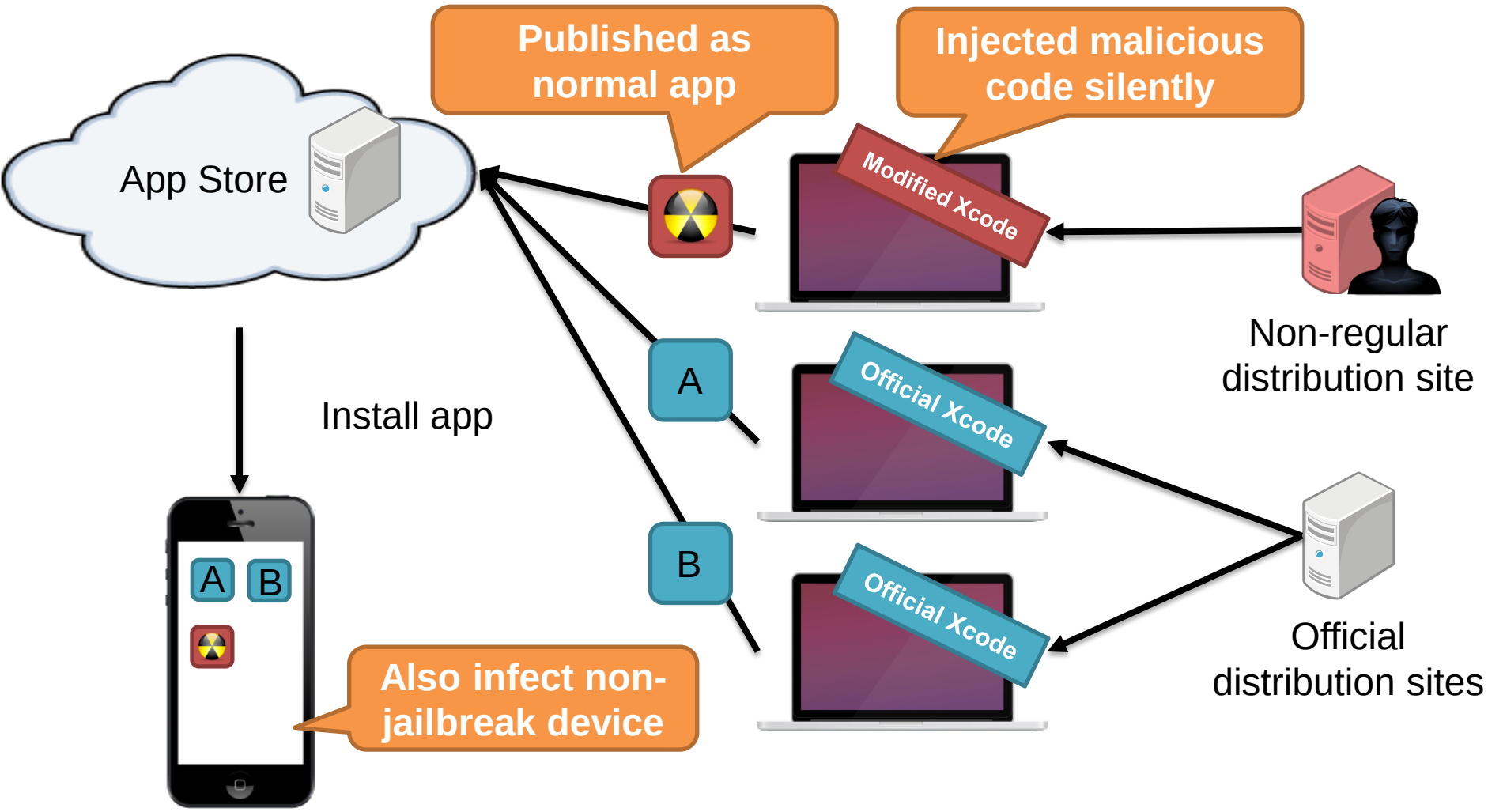
Introduction

- New malware diffusion by malicious development environment or SDK which contains the backdoor were discovered in the second half of 2015.
- Mobile app developers released own app that was injected malicious code into the market by such attacks insidiously.
- Malicious iOS apps passed review of App Store and users had installed them.
- In this report, we introduce countermeasures based on the some cases.

About XcodeGhost

- A Chinese iOS app developer customized the Xcode to add common function automatically into own app when building app.
- It was uploaded to Baidu Cloud for personal use. But it was shared to public.
  It has been diffused since download from official Xcode distribution sites was too slow in china.
- The customized Xcode added functions which steal information, clipboard, and popup ads to many apps.
- Those apps called “XcodeGhost” passed review of App Store.

About XcodeGhost



Details of XcodeGhost

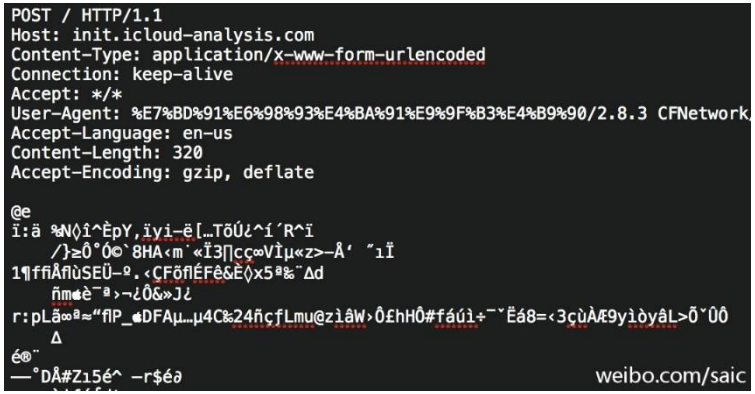
- Author of XcodeGhost said “It is just test code. So, it doesn't steal your sensitive information" on Weibo.

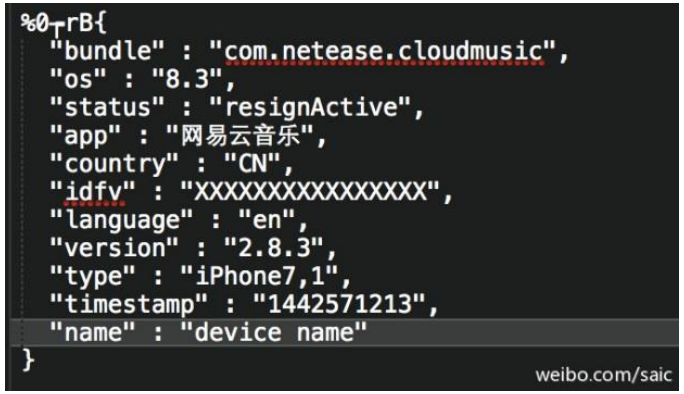
- And he showed the innocence by to publish source code on GitHub and stop the server and delete data.
  - And security research teams analyzed it.

- **Malicious functions**
  - Stealing basic information, Popup ads, install new malware, steal data of clipboard, etc.
  - Show these details below.

Details of XcodeGhost

- **Stealing basic information**
  - XcodeGhost steal below information, but it's not sensitive.
    - app name, app numbers, system version, language, country, developer symbol, install date, device name, device type
  - These information was not send to server if iOS version 9.0 or above.
    - It can't connect to non-SSL server because it did not set domain exception of ATS (App Transport Security)





http://www.weibo.com/p/1001603888503866975286

Details of XcodeGhost

- **Popup ads**
  - It's possible to pop up any ads any time for stealing payment information or Apple ID.

    And it's possible to use for installing new malware.

```
v66 = objc_msgSend(DWORD3(v120), paObjectforkey, CFSTR("alertHeader"));
v108 = objc_retainAutoreleasedReturnValue(v66);
v67 = objc_msgSend(DWORD3(v120), paObjectforkey, CFSTR("alertBody"));
LODWORD(v120) = objc_retainAutoreleasedReturnValue(v67);
v68 = objc_msgSend(DWORD3(v120), paObjectforkey, CFSTR("appID"));
v119 = objc_retainAutoreleasedReturnValue(v68);
v69 = objc_msgSend(DWORD3(v120), paObjectforkey, CFSTR("cancelTitle"));
v110 = objc_retainAutoreleasedReturnValue(v69);
v70 = objc_msgSend(DWORD3(v120), paObjectforkey, CFSTR("confirmTitle"));
v124 = objc_retainAutoreleasedReturnValue(v70);
v71 = objc_msgSend(&OBJC_CLASS___UIApplication, paSharedapplicat);
```

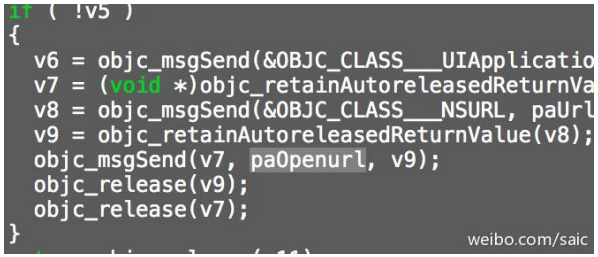


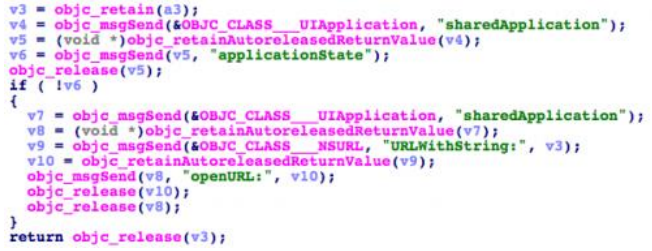
```
v115 = v45;
v122 = (char *)CFSTR("configUrl") + v45 - 4906;
v75 = objc_msgSend(v42, v46, v122);
v76 = objc_retainAutoreleasedReturnValue(v75);
if ( v76 )
{
  v77 = objc_msgSend(v42, v46, (char *)CFSTR("scheme") + v115 - 4906);
  v123 = v42;
  v78 = objc_retainAutoreleasedReturnValue(v77);
```


http://www.weibo.com/p/1001603888503866975286

Details of XcodeGhost

- **Install new malware**
  - It's possible to install new malware from any place using "pop up ads" function or URL scheme.
  - One of the reason to pass review of App Store, is that to send the information that can get by common API or to open arbitrary URL is not problem only it.
  - However XcodeGhost could install another malware which signed by iDEP (iOS Developer Enterprise Program) in the function.





http://www.weibo.com/p/1001603888503866975286

http://researchcenter.paloaltonetworks.com/2015/09/update-xcodeghost-attacker-can-phish-passwords-and-open-urls-though-infected-apps/

Details of XcodeGhost

- **Steal clipboard data**
  - XcodeGhost saves and sends clipboard data.
    (It works only in the infected app)
  - However dropped malware could work background and steal all app's clipboard.

A case in Android

- **Moplus**
  - Moplus developed by baidu included backdoor.
  - Infected 14,112 apps
  - 4014 apps of infected apps were published in “com.baidu.appsearch” as baidu official app.

    And total downloads numbers are over 1 billion.

http://blog.trendmicro.co.jp/archives/12540

Concerns of new attack

- **Attack to Embedded Framework**
  - Embedded Framework added at iOS 8.
  - It is possible to execute code dynamically.
  - Some apps use it like adding useful functions.
  - It can be considered an attack such as Moplus.

- **Attack to development environment modules**
  - It's possible to steal source code or to add malicious code by inject malicious code into module that was added to the efficiency of coding.

Countermeasures for developers

- **Don't use untrusted "SDK", "development environment", "development environment modules“**
  - If you have to use them, you should checking added malicious functions for example "external communication", "Permission Requests", "Access to user data".

- **Monitoring app traffic before release**
  - Check suspicious communication.
  - Malware usually send data to server.

Countermeasures for users

- **Don't install app from non-official market**
  - Case in official market, security researchers found malicious app like "XcodeGhost" or "Moplus" by to focus official market.
  - But we can't analyze all apps in non-official market.
  - There are high risk apps to be infected malware in non-official market.

- **Don't install untrusted apps except managed by yourself**
  - Most of existing malware use untrusted signature or market.

Summary

- The diffusion of malware from official store is there in both iOS and Android.

- In recent cases, malicious development environment and SDK were being exploited in malware diffusion.
  As a result, Non-malicious developers had diffused malware.

- To counter these threats, there is a thing to be aware of developers and users.

References

- XcodeGhost 实际用途猜测分析 - 文章
  http://www.weibo.com/p/1001603888503866975286

- #XcodeGhost#关于所谓"XcodeGhost"的澄清。... 来自XcodeGhost-Author - 微博
  http://www.weibo.com/5704632164/CBc4S9H9p?from=page_1005055704632164_profile&wvr=6&mod=weibotime&type=comment#_rnd1452219037152

- 不具合を抱えるMoplus SDK、Baidu 以外のアプリにも影響 | トレンドマイクロ セキュリティブログ
  http://blog.trendmicro.co.jp/archives/12566

- 脆弱性を抱えるソフトウェア開発キット「Moplus」、実はバックドア機能の実装が判明 | トレンドマイクロ セキュリティブログ
  http://blog.trendmicro.co.jp/archives/12540

Contact Information

E-Mail ： research—feedback@ffri.jp
Twitter： @FFRI_Research