/Rooted 2016

A Journey through iOS Malware Landscape

Evolution & Characterization

Laura García[1] & Ricardo J. Rodríguez[2]

[1] Planet Earth
[2] University of Zaragoza, Spain

>whoami

Laura García

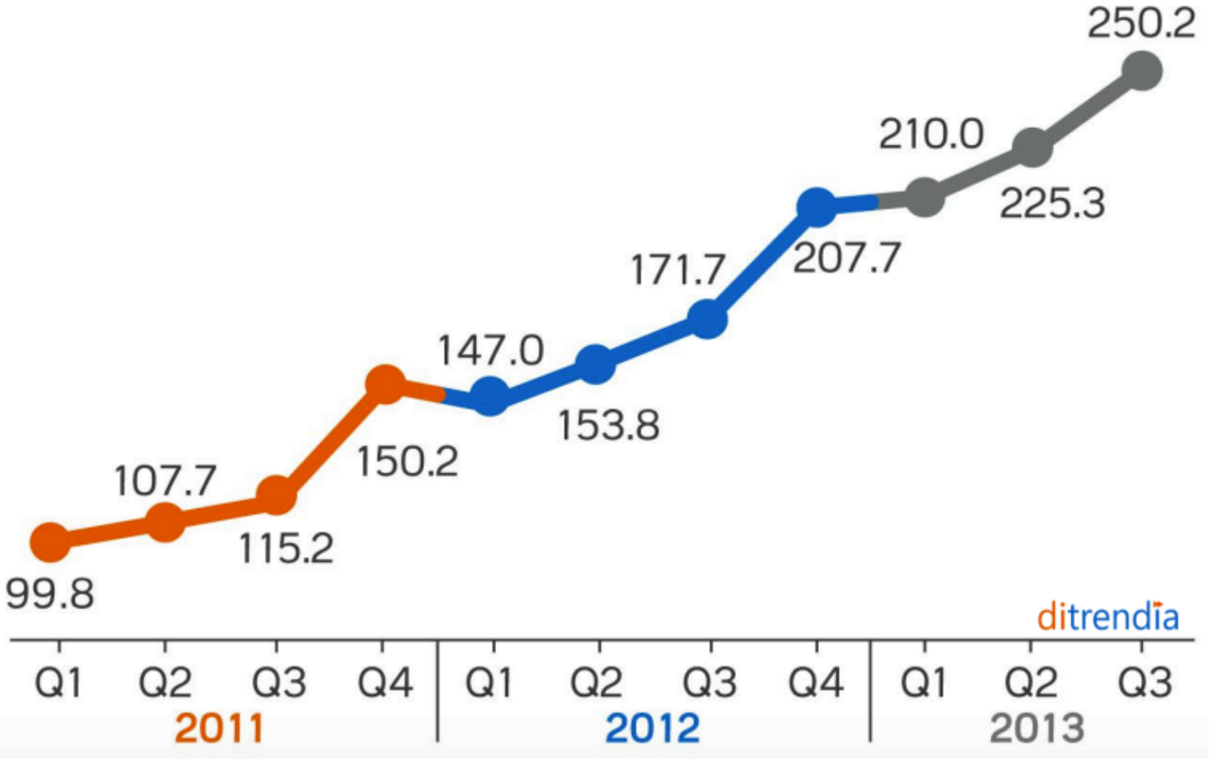
- Computer Science Engineering
- Master's Degree in Computer Security
- ^Cyber^ Security / Pentester
- Web and mobile app security, vulnerability assessment, network security, system hardening and incident response
- github.com/laincode
- laura@mlw.re

Ricardo J. Rodríguez

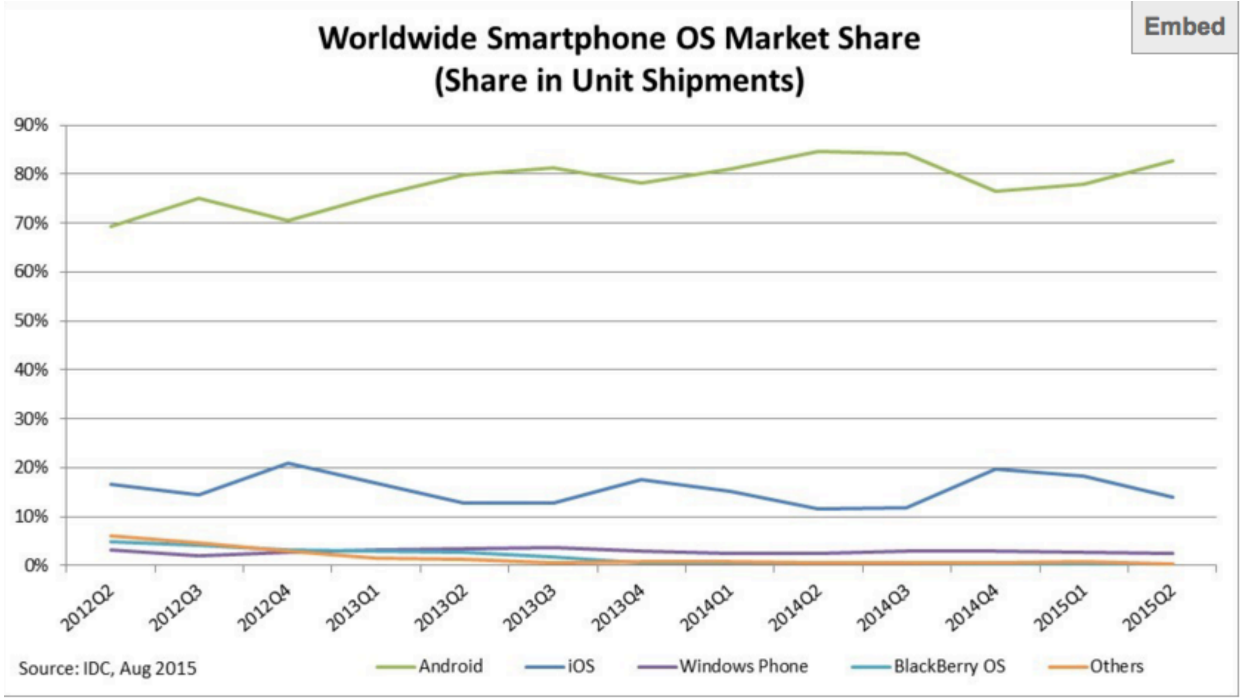
- PhD in Computer Science
- Assistant Professor at University of Zaragoza
- Performance analysis and optimization of large and complex systems, program binary analysis, critical infrastructures security
- bitbucket.org/rjrodriguez
- rjrodriguez@unizar.es

1. Introduction

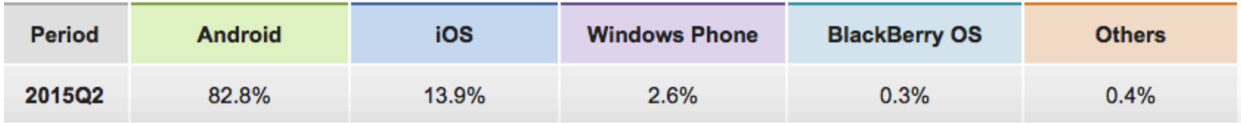
1. Introduction (I)



1. Introduction (II)



Source: IDC, Aug 2015



Period	Android	iOS	Windows Phone	BlackBerry OS	Others
2015Q2	82.8%	13.9%	2.6%	0.3%	0.4%

1. Introduction (III)

- Android OS clearly beats the market
- Consequently, there exist a large set of malware for Android
  - Last report from Forbes: 97% target at Android
    http://www.forbes.com/sites/gordonkelly/2014/03/24/report-97-of-mobile-malware-is-on-android-this-is-the-easy-way-you-stay-safe/#768449637d53
    - 238 in 2012 to 804 in 2013 (...)

1. Introduction (IV)

- Keep an eye on this table:

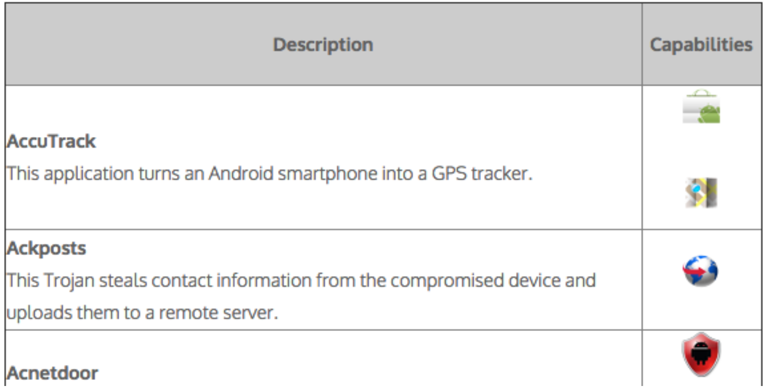
  http://forensics.spreitzenbarth.de/android-malware/

  – 200 families (roughly)

  – Bots, PUPs, fraud, …

- Tons of tools & defence mechanisms proposed

  – As well as taxonomies



Description	Capabilities
AccuTrack This application turns an Android smartphone into a GPS tracker.	
Ackposts This Trojan steals contact information from the compromised device and uploads them to a remote server.	
Acnetdoor	

1. Introduction (V)

- What about iOS malware?
  https://www.theiphonewiki.com/wiki/Malware_for_iOS
  - Few (known) families (~35)
  - Less attention from the academia. How come?
    - Market share: the higher the number of devices, the greater the probability of success of infection
    - Security models differ
      - Permission-based approach (differ on granularity) + platform protection mechanisms (ASLR, DEP)
      - Unlike Android, iOS relies also on market protection

1. Introduction (VI)

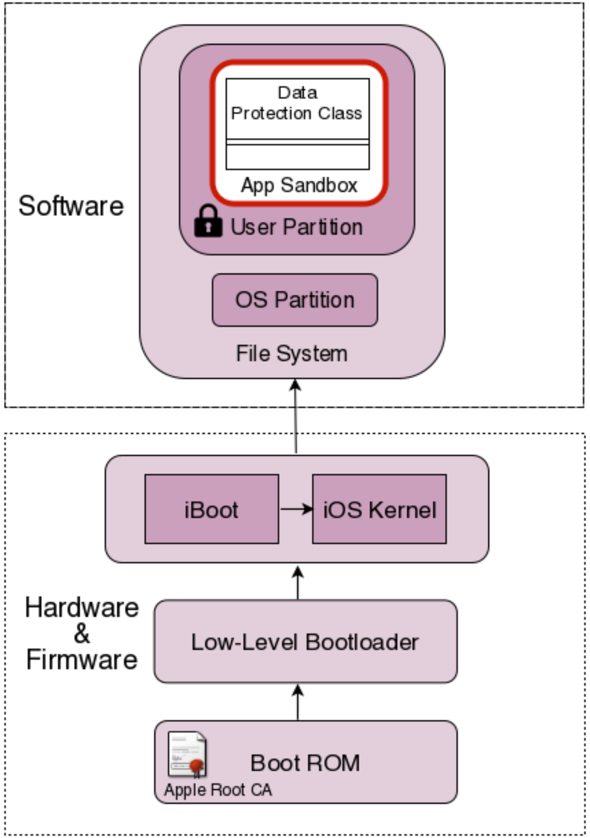
- Apple vetting process
  - Apps must comply a set of rules before deployment to final users (thr. official markets)
- Effective, but…
  - XCodeGhost: trojanized official SDK
    - 39 malware apps into the App Store during last year
  - Other: enterprise/ad-hoc provisioning, private APIs abuse, compromised iCloud accounts

1. Introduction (VII)

- Taxonomy and classification of 35 iOS malware families (2009 to 2015), regarding:
  - Affected devices
  - Distribution channels
  - Infection
  - Attack goals
  - Attack vector

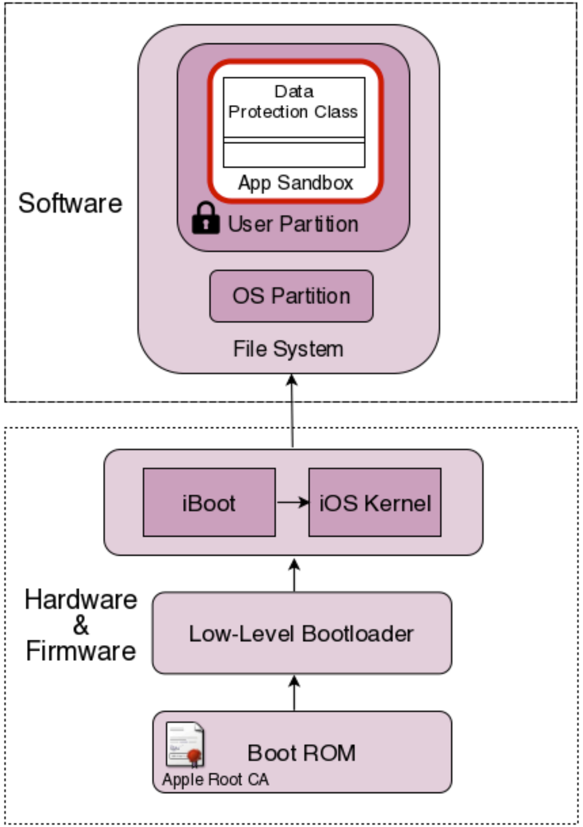
2. On iOS Security Model

2. On iOS Security Model (I): iOS architecture



- Secure boot chain
  - Integrity of low-level code
  - Execution upon a valid device
- Boot ROM
  - Immutable code
  - Contains Apple Root CA pk
    - Used to verify LLB signature

2. On iOS Security Model (II): iOS architecture



- Low-Level Bootloader (LLB)
  - Verifies and executes iBoot
- iBoot
  - Verifies and executes iOS kernel
- iOS Kernel
  - Verifies and executes full iOS
  - Loads OS + user partition
- NOTE: firmware is signed

2. On iOS Security Model (III): iOS architecture

- Different app security layers
  - Apple-issued certificate
    - Every app is signed by developers using a certificate issued by Apple, after identity verification thr. iOS Dev Program
  - App sandbox: isolated, non-privileged user "mobile"
  - Data Protection
    - Data file associated with a specific class file, defining access granularity
  - Others: ASLR, DEP

2. On iOS Security Model (IV): vetting process

- App Review Guidelines (https://developer.apple.com/app-store/review/guidelines/)
- Ensures apps...
  - Are reliable
  - Perform as expected
  - Free of any offensive material
- Set of over 100 rules, covering aspects as functionality, meta-data, location, advertising, etc.

2. On iOS Security Model (V): vetting process

- Reasons to reject submitted apps:
  - Crash on execution
  - Inclusion of undocumented/hidden features
  - Use of private APIs
  - Data read or write out of boundaries
  - Download any external code
- Bypassing examples:
  - trojanized SDK, obfuscate private APIs, abuse of inter-app interaction services

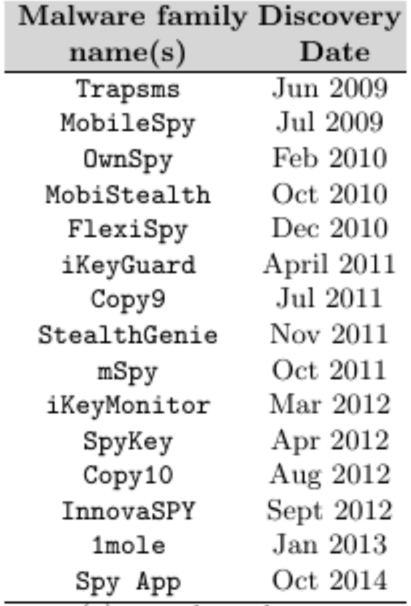
3. Features of iOS malware

3. Features of iOS malware (I)

Who are targeting at individuals?

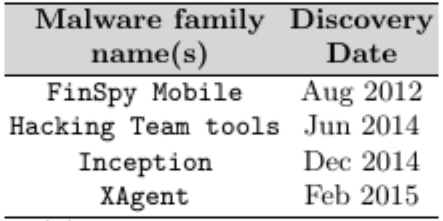
- On-sale malware
  - For sale to the public (any of you folks!)
- State-sponsored malware
  - Government/state intelligence agencies
- Underground malware
  - Cybercriminals -- aka *malware in-the-wild*

3. Features of iOS malware (II)



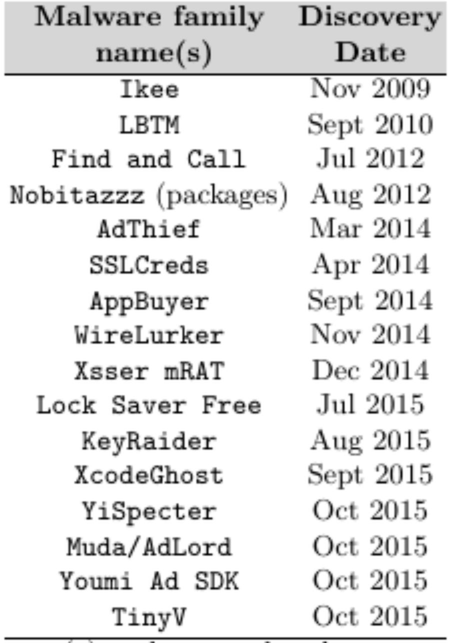
Malware family name(s)	Discovery Date
Trapsms	Jun 2009
MobileSpy	Jul 2009
OwnSpy	Feb 2010
MobiStealth	Oct 2010
FlexiSpy	Dec 2010
iKeyGuard	April 2011
Copy9	Jul 2011
StealthGenie	Nov 2011
mSpy	Oct 2011
iKeyMonitor	Mar 2012
SpyKey	Apr 2012
Copy10	Aug 2012
InnovaSPY	Sept 2012
1mole	Jan 2013
Spy App	Oct 2014

(a) on-sale malware



Malware family name(s)	Discovery Date
FinSpy Mobile	Aug 2012
Hacking Team tools	Jun 2014
Inception	Dec 2014
XAgent	Feb 2015

(b) state-sponsored malware

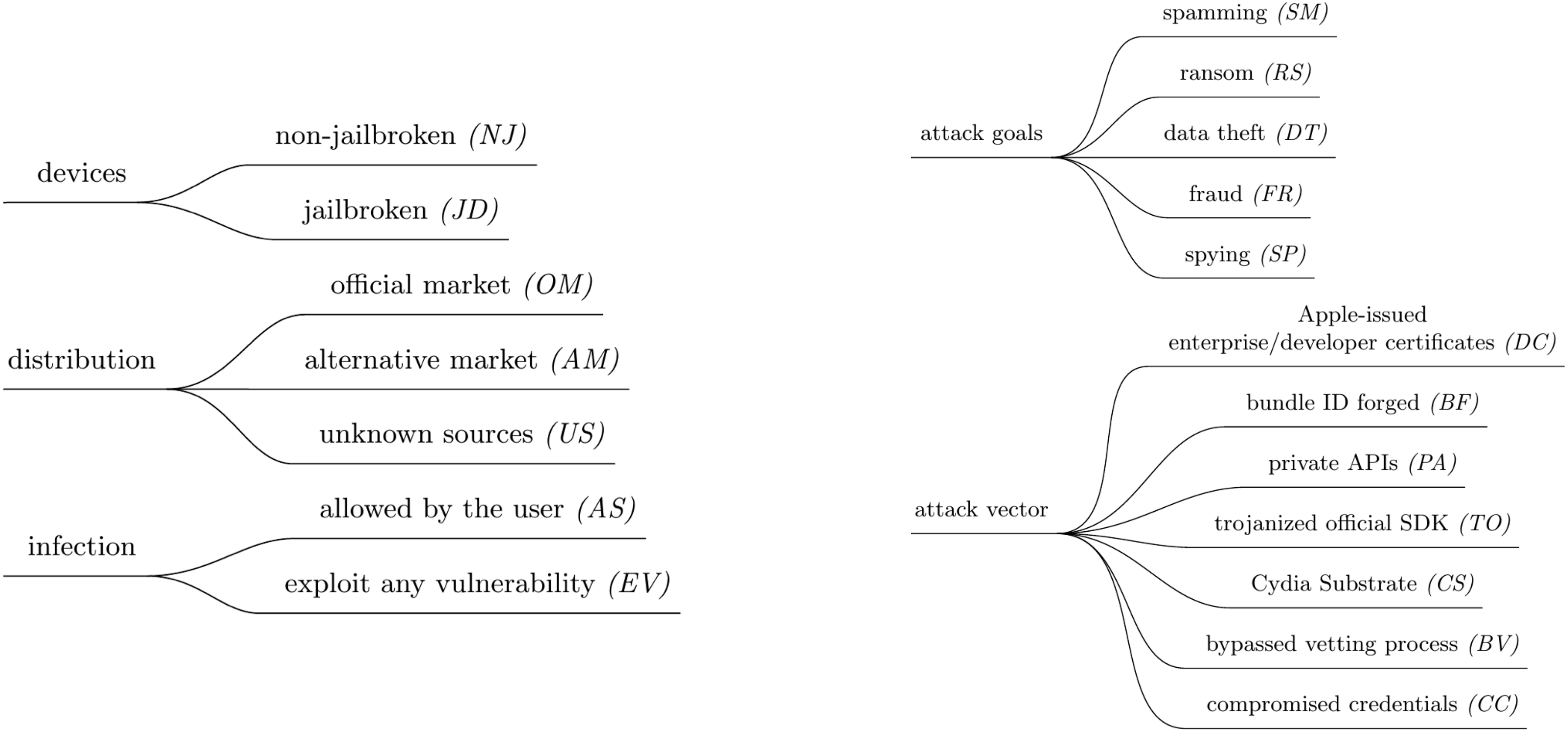


Malware family name(s)	Discovery Date
Ikee	Nov 2009
LBTM	Sept 2010
Find and Call	Jul 2012
Nobitazzz (packages)	Aug 2012
AdThief	Mar 2014
SSLCreds	Apr 2014
AppBuyer	Sept 2014
WireLurker	Nov 2014
Xsser mRAT	Dec 2014
Lock Saver Free	Jul 2015
KeyRaider	Aug 2015
XcodeGhost	Sept 2015
YiSpecter	Oct 2015
Muda/AdLord	Oct 2015
Youmi Ad SDK	Oct 2015
TinyV	Oct 2015

(c) underground malware

15+4+16 malware families, from 2009 to 2015

3. Features of iOS malware (III)

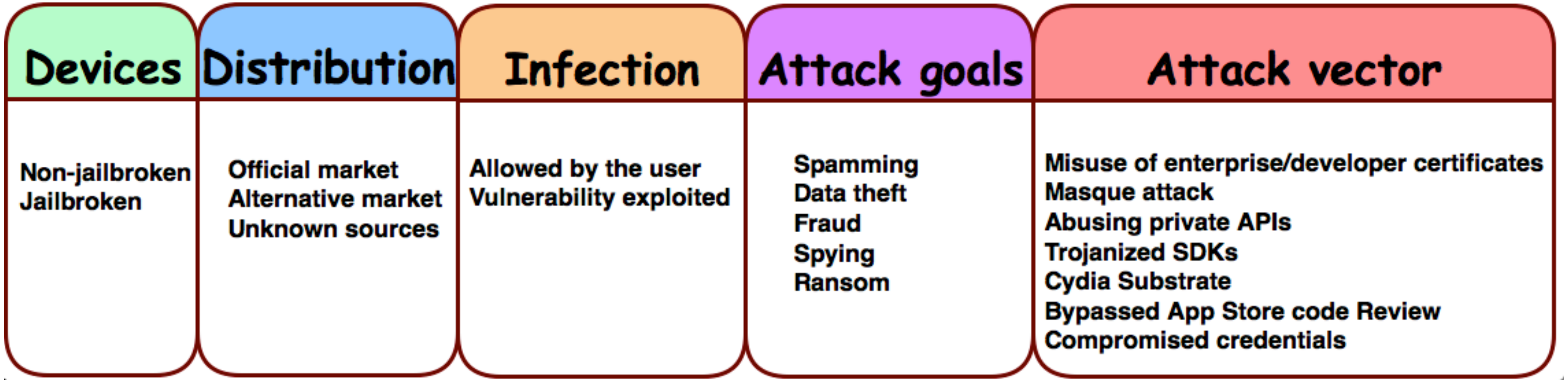


- devices
  - non-jailbroken *(NJ)*
  - jailbroken *(JD)*
- distribution
  - official market *(OM)*
  - alternative market *(AM)*
  - unknown sources *(US)*
- infection
  - allowed by the user *(AS)*
  - exploit any vulnerability *(EV)*
- attack goals
  - spamming *(SM)*
  - ransom *(RS)*
  - data theft *(DT)*
  - fraud *(FR)*
  - spying *(SP)*
- attack vector
  - Apple-issued enterprise/developer certificates *(DC)*
  - bundle ID forged *(BF)*
  - private APIs *(PA)*
  - trojanized official SDK *(TO)*
  - Cydia Substrate *(CS)*
  - bypassed vetting process *(BV)*
  - compromised credentials *(CC)*

4. Classification of iOS malware

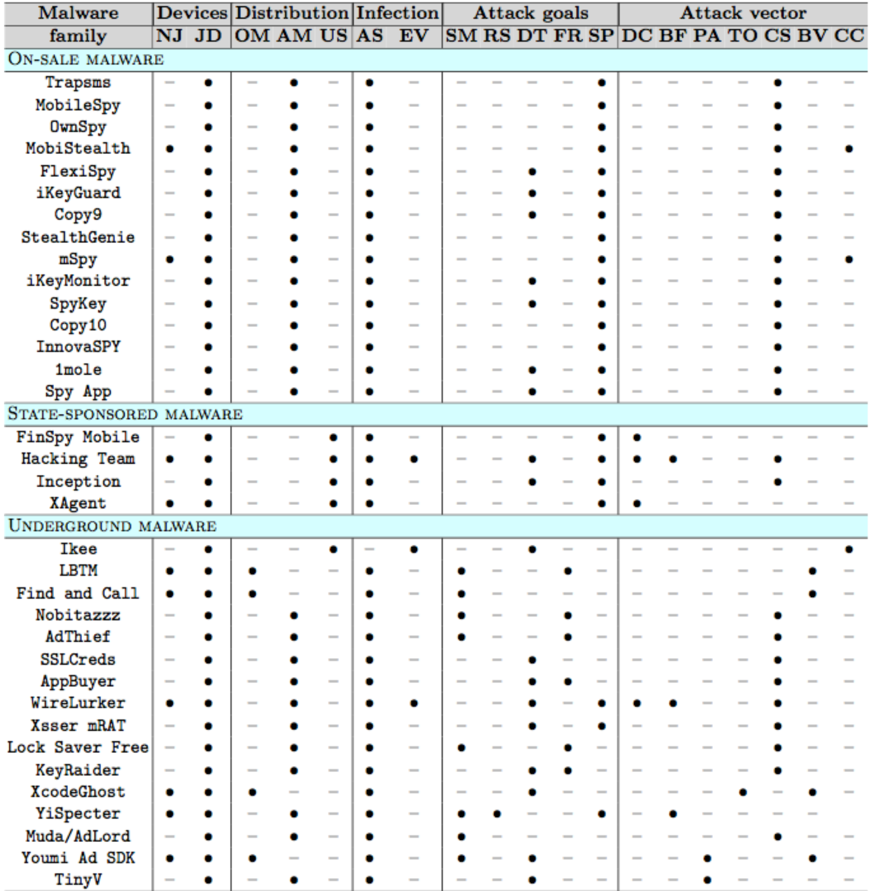
4. Classification of iOS malware (I)

Classification a total of **35 malware families** according to the next features:



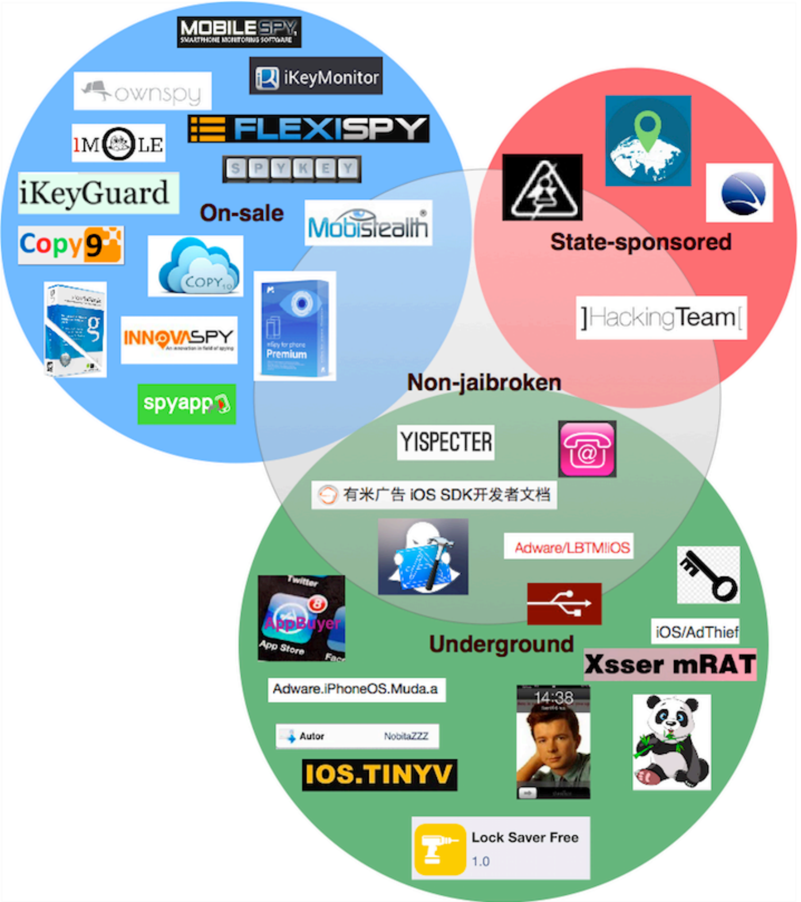
Devices	Distribution	Infection	Attack goals	Attack vector
Non-jailbroken Jailbroken	Official market Alternative market Unknown sources	Allowed by the user Vulnerability exploited	Spamming Data theft Fraud Spying Ransom	Misuse of enterprise/developer certificates Masque attack Abusing private APIs Trojanized SDKs Cydia Substrate Bypassed App Store code Review Compromised credentials

4. Classification of iOS malware (II)



Malware	Devices		Distribution			Infection		Attack goals					Attack vector						
family	NJ	JD	OM	AM	US	AS	EV	SM	RS	DT	FR	SP	DC	BF	PA	TO	CS	BV	CC
ON-SALE MALWARE																			
Trapsms	–	●	–	●	–	●	–	–	–	–	–	●	–	–	–	–	●	–	–
MobileSpy	–	●	–	●	–	●	–	–	–	–	–	●	–	–	–	–	●	–	–
OwnSpy	–	●	–	●	–	●	–	–	–	–	–	●	–	–	–	–	●	–	–
MobiStealth	●	●	–	●	–	●	–	–	–	–	–	●	–	–	–	–	●	–	●
FlexiSpy	–	●	–	●	–	●	–	–	–	●	–	●	–	–	–	–	●	–	–
iKeyGuard	–	●	–	●	–	●	–	–	–	●	–	●	–	–	–	–	●	–	–
Copy9	–	●	–	●	–	●	–	–	–	●	–	●	–	–	–	–	●	–	–
StealthGenie	–	●	–	●	–	●	–	–	–	–	–	●	–	–	–	–	●	–	–
mSpy	●	●	–	●	–	●	–	–	–	–	–	●	–	–	–	–	●	–	●
iKeyMonitor	–	●	–	●	–	●	–	–	–	●	–	●	–	–	–	–	●	–	–
SpyKey	–	●	–	●	–	●	–	–	–	●	–	●	–	–	–	–	●	–	–
Copy10	–	●	–	●	–	●	–	–	–	–	–	●	–	–	–	–	●	–	–
InnovaSPY	–	●	–	●	–	●	–	–	–	–	–	●	–	–	–	–	●	–	–
1mole	–	●	–	●	–	●	–	–	–	●	–	●	–	–	–	–	●	–	–
Spy App	–	●	–	●	–	●	–	–	–	●	–	●	–	–	–	–	●	–	–
STATE-SPONSORED MALWARE																			
FinSpy Mobile	–	●	–	–	●	●	–	–	–	–	–	●	●	–	–	–	–	–	–
Hacking Team	●	●	–	–	●	●	●	–	–	●	–	●	●	●	–	–	●	–	–
Inception	–	●	–	–	●	●	–	–	–	●	–	●	–	–	–	–	●	–	–
XAgent	●	●	–	–	●	●	–	–	–	–	–	●	●	–	–	–	–	–	–
UNDERGROUND MALWARE																			
Ikee	–	●	–	–	●	–	●	–	–	●	–	–	–	–	–	–	–	–	●
LBTM	●	●	●	–	–	●	–	●	–	–	●	–	–	–	–	–	–	●	–
Find and Call	●	●	●	–	–	●	–	●	–	–	–	–	–	–	–	–	–	●	–
Nobitazzz	–	●	–	●	–	●	–	●	–	–	●	–	–	–	–	–	●	–	–
AdThief	–	●	–	●	–	●	–	●	–	–	●	–	–	–	–	–	●	–	–
SSLCreds	–	●	–	●	–	●	–	–	–	●	–	–	–	–	–	–	●	–	–
AppBuyer	–	●	–	●	–	●	–	–	–	●	●	–	–	–	–	–	●	–	–
WireLurker	●	●	–	●	–	●	●	–	–	●	–	●	●	●	–	–	●	–	–
Xsser mRAT	–	●	–	●	–	●	–	–	–	●	–	●	–	–	–	–	●	–	–
Lock Saver Free	–	●	–	●	–	●	–	●	–	–	●	–	–	–	–	–	●	–	–
KeyRaider	–	●	–	●	–	●	–	–	–	●	●	–	–	–	–	–	●	–	–
XcodeGhost	●	●	●	–	–	●	–	–	–	●	–	–	–	–	–	●	–	●	–
YiSpecter	●	●	–	●	–	●	–	●	●	–	–	●	–	●	–	–	–	–	
Muda/AdLord	–	●	–	●	–	●	–	●	–	–	–	–	–	–	–	–	●	–	–
Youmi Ad SDK	●	●	●	–	–	●	–	●	–	●	–	–	–	–	●	–	–	●	–
TinyV	–	●	–	●	–	●	–	–	–	●	–	–	–	–	●	–	–	–	–

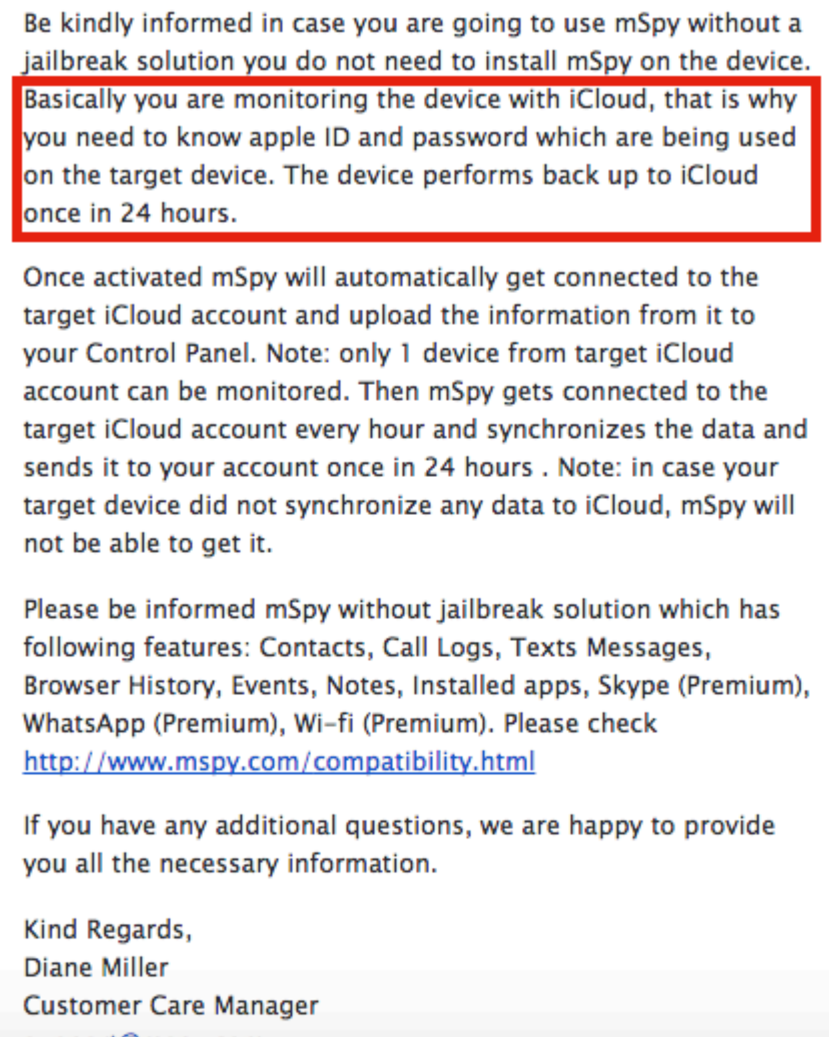
4. Classification of iOS malware (III)



Devices

- Few work on non-jailbroken devices
- Many of them require jailbroken devices
- **Jailbreaking increases the likelihood to be infected**
- Cydia allows anyone to run a third-party repository and distribute any software
- Mostly spyware tools require jailbroken devices
- *“Finding may **secretly jailbreak** the target's device”*

  -The Million Dollar **iOS 9 Bug Bounty**-
- Some malware run old iOS versions, but do not work on current ones



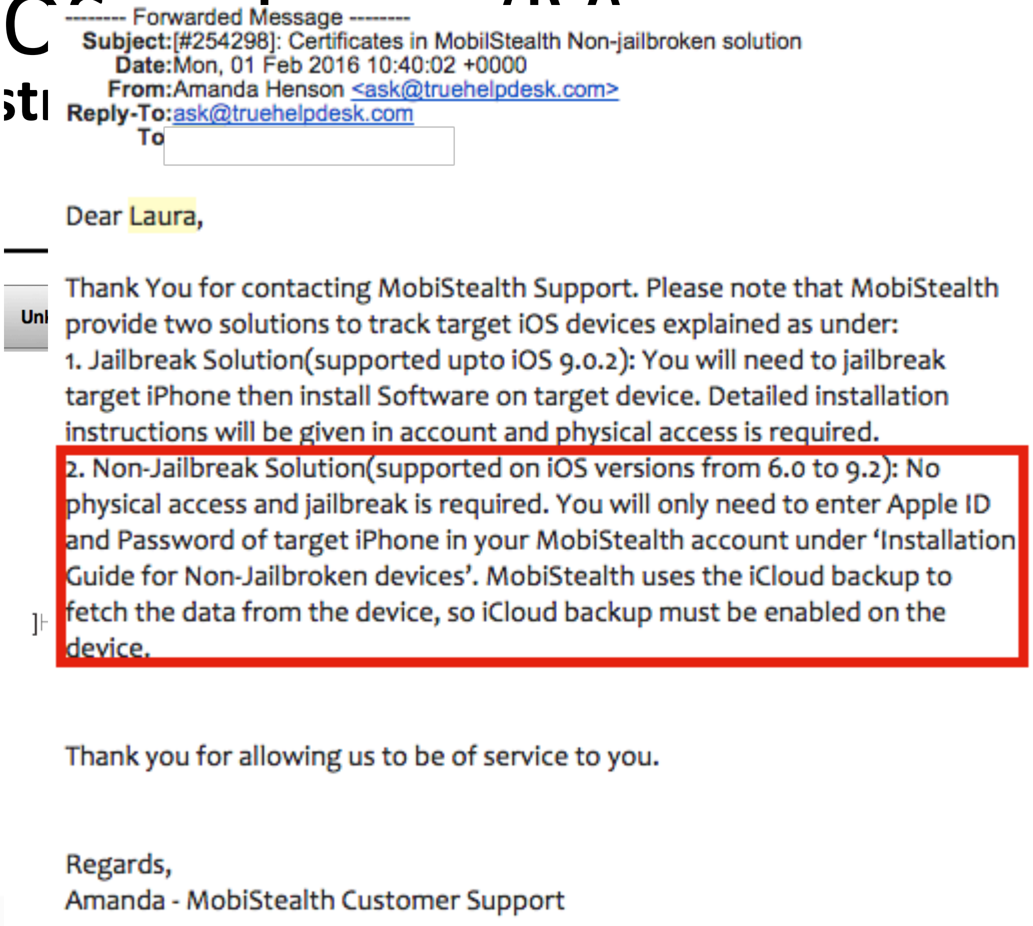
Be kindly informed in case you are going to use mSpy without a jailbreak solution you do not need to install mSpy on the device. Basically you are monitoring the device with iCloud, that is why you need to know apple ID and password which are being used on the target device. The device performs back up to iCloud once in 24 hours.

Once activated mSpy will automatically get connected to the target iCloud account and upload the information from it to your Control Panel. Note: only 1 device from target iCloud account can be monitored. Then mSpy gets connected to the target iCloud account every hour and synchronizes the data and sends it to your account once in 24 hours . Note: in case your target device did not synchronize any data to iCloud, mSpy will not be able to get it.

Please be informed mSpy without jailbreak solution which has following features: Contacts, Call Logs, Texts Messages, Browser History, Events, Notes, Installed apps, Skype (Premium), WhatsApp (Premium), Wi-fi (Premium). Please check http://www.mspy.com/compatibility.html

If you have any additional questions, we are happy to provide you all the necessary information.

Kind Regards,
Diane Miller
Customer Care Manager



-------- Forwarded Message --------
Subject:[#254298]: Certificates in MobilStealth Non-jailbroken solution
Date: Mon, 01 Feb 2016 10:40:02 +0000
From: Amanda Henson <ask@truehelpdesk.com>
Reply-To:ask@truehelpdesk.com
To

Dear Laura,

Thank You for contacting MobiStealth Support. Please note that MobiStealth provide two solutions to track target iOS devices explained as under:
1. Jailbreak Solution(supported upto iOS 9.0.2): You will need to jailbreak target iPhone then install Software on target device. Detailed installation instructions will be given in account and physical access is required.
2. Non-Jailbreak Solution(supported on iOS versions from 6.0 to 9.2): No physical access and jailbreak is required. You will only need to enter Apple ID and Password of target iPhone in your MobiStealth account under 'Installation Guide for Non-Jailbroken devices'. MobiStealth uses the iCloud backup to fetch the data from the device, so iCloud backup must be enabled on the device.

Thank you for allowing us to be of service to you.

Regards,
Amanda - MobiStealth Customer Support

4. Classification of iOS malware (V)

Infection

User’s fault by installing the malicious App

- **Cydia Apps** & **extensions**
  - 75000 devices infected with AdThief/Spad
  - 225k valid Apple accounts compromised with KeyRaider
- **App Store**
  - At least 39 apps published in the iOS App Store with XcodeGhost
  - 256 apps (~1M downloads) affected with Youmi Ad SDK
- **Underground websites**
- **Social engineering** (or other) delivery
- **Via USB** with an infected computer
  - Hundreds of thousands affected devices (mostly in China) with WireLurker

Third-party **user’s credentials**

4. Classification of iOS malware (VI)

Infection

Few cases involve exploiting a vulnerability in the device

- **CVE-2014-1276** (fixed in iOS 7.1)
  - **Monitor** on **user actions** in other apps
- **Date Trick** (fixed in iOS 8.1)
  - **Expired** enterprise **certificates**, by user to set the device's time back
- **CVE-2014-4494** (fixed in iOS 8.1)
  - Enterprise-signed app launched **without prompting for trust**
- **CVE-2014-4493** (fixed in iOS 8.1.3)
  - Enterprise-signed application may be able to **take control of the local container** for applications
- **CVE-2015-3722**, **CVE-2015-3725** (Masque Attack, fixed in iOS 8.4)
  - Allowed a **collision** to occur with **existing bundle IDs**
- **CVE-2015-5770** (fixed in iOS 8.4.1)
  - Does not ensure the **uniqueness** of universal provisioning **profile bundle IDs**

]HackingTeam[

4. Classification of iOS malware (VII)

Attack goals

On-sale and **state-sponsored** malware mainly focused on **spying** and **data theft** (as expected!)

- SMS, iMessage, Emails, Call Logs, GPS Location, Key presses, Skype, WhatsApp, Viber, Facebook, Images, Videos, listen in real time actual phone calls
- **FinSpy**: Recording of common communications. File download. Country tracing of target
- **Hacking Team**:
  - *Remote Control System tool* for monitoring of chat, location, contacts, and list of calls
  - *Newsstand keylogger tool* capture keystrokes
  - *11 iOS apps within Hacking Team's arsenals that utilise Masque Attack*

- **Inception:** Capturing user's address book, phone number, roaming status, AppleID, MAC address, Wifi status, default and local time zone and more
- **Operation Pawn Storm:**
  - *XAgent* steals personal data, record audio, make screenshots
  - *Madcap* is similar to the XAgent malware, but unlike it, MadCap is focused on recording audio

4. Classification of iOS malware (VIII)

Attack goals

Top 5 attack goals in **Underground** malware

1. **Data theft**

   Stealing Apple IDs

   - KeyRaider: stolen **Apple ID** accounts
   - SSLCreds / Unflod Baby Panda: listens to outgoing SSL connections and steal **Apple ID** credentials
   - XcodeGhost: create fake **iCloud password** sign-in prompts, UUID, device name
   - WireLurker: Information stealing (contact names phone numbers, **Apple ID**, UDID)

2. **Spamming**

   Stealing revenue from **advertisments**

   - AdThief/Spad: **hijack the revenues** fro **ements** on the infected device. The hooks modify the publisher identifier and generate revenue for the attacker referenced by the modified identifier
   - Lock Saver Free: extra tweak that hooks into ad banners to insert its own ad identifier, presumably in order to **give ad revenue** to the author of the tweak

4. Classification of iOS malware (IX)

Attack goals

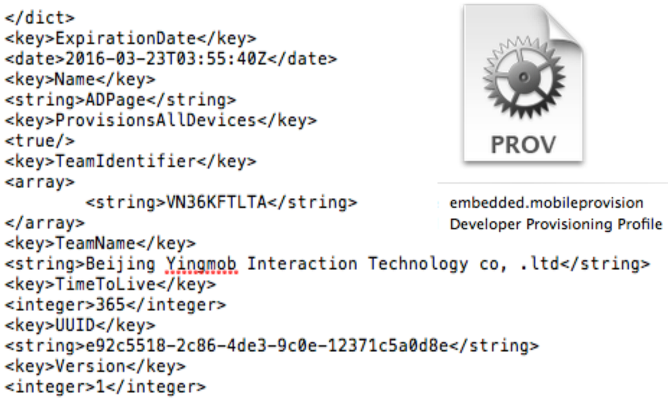
3. **Commit fraud**
   - AppBuyer: steal user's Apple ID and password and buy apps from the official App Store by victim's identity
   - KeyRaider: attackers can purchase non-free iOS apps from App Store using stolen accounts
4. **Spying**
   - mRAT: used against the Occupy Central protesters in Hong Kong ("WhatsApp msg with link"). Extract a vast range of personal information including iOS address book, SMS messages, call logs, GSM identities, **geographical location** (by the **cell tower ID**), on-device pictures, as well as passwords and other authentication data in the iOS keychains
5. **Ransom**
   - KeyRaider: also has built-in functionality to **hold iOS devices** for ransom
   - Previous ransomware attacks: remotely controlling the iOS device through the iCloud service (Find my Phone)

4. Classification of iOS malware (X)

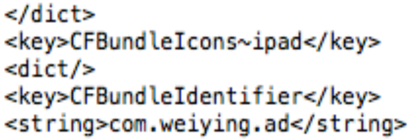
Attack vector

Attacking non-jailbroken devices

- **Misuse of enterprise and developer certificates**
  - WireLurker installs downloaded third-party applications
  - Hacking Team has a legitimate signing certificate
  - YiSpecter download its components signed with enterprise certificate
  - Released **iOS 9 has been improved** enterprise cert
- **Masque attack**
  - Could replace a legitimate application as long as both applications used the **same bundle identifier.**
  - A bundle ID precisely identifies a single application
  - WireLurker replace another genuine app as long as both apps used the same bundle identifier.
  - Hacking Team was re-packaging apps such as Skype, Twitter, Facebook, WhatsApp and more.



```
</dict>
<key>ExpirationDate</key>
<date>2016-03-23T03:55:40Z</date>
<key>Name</key>
<string>ADPage</string>
<key>ProvisionsAllDevices</key>
<true/>
<key>TeamIdentifier</key>
<array>
        <string>VN36KFTLTA</string>
</array>
<key>TeamName</key>
<string>Beijing Yingmob Interaction Technology co, .ltd</string>
<key>TimeToLive</key>
<integer>365</integer>
<key>UUID</key>
<string>e92c5518-2c86-4de3-9c0e-12371c5a0d8e</string>
<key>Version</key>
<integer>1</integer>
```



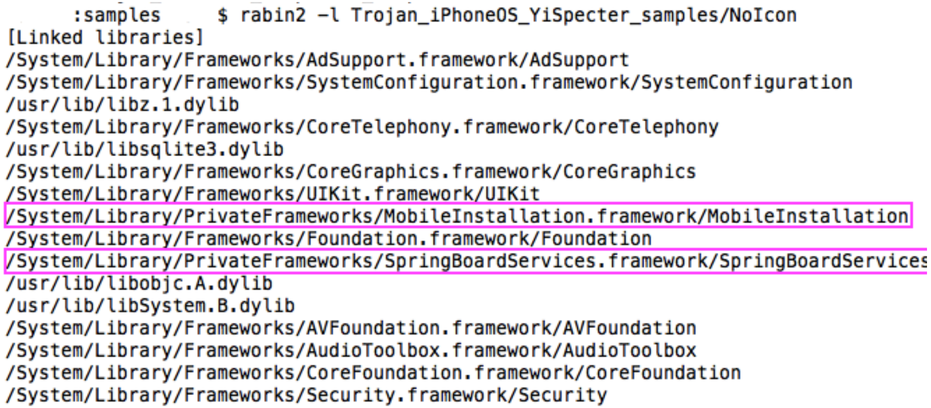
```
</dict>
<key>CFBundleIcons~ipad</key>
<dict/>
<key>CFBundleIdentifier</key>
<string>com.weiying.ad</string>
```

4. Classification of iOS malware (XI)

Attack vector

Attacking non-jailbroken devices (cont.)

- **Abusing private APIs**
    - **Undocumented API** of the iOS frameworks
    - Used to **implement sensitive functionalities** and **steal sensitive information**
    - Youmi Ad SDK steals user's Apple ID email address, platform serial
    - YiSpecter combines enterprise certificates to get installed in devices and abuse private APIs to **download and install** each component
    - TinyV abuse private APIs to **download and install** components
    - Security researchers have focused how to scan for private API usage (SourceDNA, CC-Tool, iRiS)



```
      :samples     $ rabin2 -l Trojan_iPhoneOS_YiSpecter_samples/NoIcon
[Linked libraries]
/System/Library/Frameworks/AdSupport.framework/AdSupport
/System/Library/Frameworks/SystemConfiguration.framework/SystemConfiguration
/usr/lib/libz.1.dylib
/System/Library/Frameworks/CoreTelephony.framework/CoreTelephony
/usr/lib/libsqlite3.dylib
/System/Library/Frameworks/CoreGraphics.framework/CoreGraphics
/System/Library/Frameworks/UIKit.framework/UIKit
/System/Library/PrivateFrameworks/MobileInstallation.framework/MobileInstallation
/System/Library/Frameworks/Foundation.framework/Foundation
/System/Library/PrivateFrameworks/SpringBoardServices.framework/SpringBoardServices
/usr/lib/libobjc.A.dylib
/usr/lib/libSystem.B.dylib
/System/Library/Frameworks/AVFoundation.framework/AVFoundation
/System/Library/Frameworks/AudioToolbox.framework/AudioToolbox
/System/Library/Frameworks/CoreFoundation.framework/CoreFoundation
/System/Library/Frameworks/Security.framework/Security
```

4. Classification of iOS malware (XII)

Attack vector

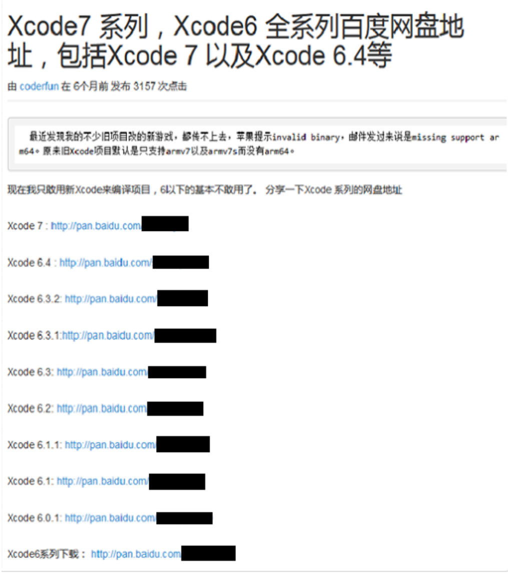
Attacking non-jailbroken devices (cont.)

- **Trojanized SDK**
  - XcodeGhost is the **first compiler malware** in OS X. Its malicious code located in a Mach-O object file repackaged into some version of Xcode

Xcode.app/.../SDKs/Library/Frameworks/CoreServices.framework/CoreService

Xcode.app/.../SDKs/Library/PrivateFrameworks/IDEBundleInjection.framework

- **Bypassing App Store code Review**
  - In addition to abuse of private APIs and trojanized SDK
  - LBTM adware (2009) and Find and Call worm (2010)
- **Compromised Credentials**
  - Apple ID credentials compromised (MobiStealth and mSpy)
  - Jailbreak devices Ikee/Eeki and Duh “alpine” SSH password



Xcode7 系列，Xcode6 全系列百度网盘地址，包括Xcode 7 以及Xcode 6.4等

由 coderfun 在 6个月前 发布 3157 次点击

```
  最近发现我的不少旧项目改的新游戏，都传不上去，苹果提示invalid binary，邮件发过来说是missing support ar
m64。原来旧Xcode项目默认是只支持armv7以及armv7s而没有arm64。
```

现在我只敢用新Xcode来编译项目，6以下的基本不敢用了。 分享一下Xcode 系列的网盘地址

Xcode 7 : http://pan.baidu.com[redacted]

Xcode 6.4 : http://pan.baidu.com/[redacted]

Xcode 6.3.2: http://pan.baidu.com/[redacted]

Xcode 6.3.1:http://pan.baidu.com/[redacted]

Xcode 6.3: http://pan.baidu.com[redacted]

Xcode 6.2: http://pan.baidu.com[redacted]

Xcode 6.1.1: http://pan.baidu.com[redacted]

Xcode 6.1: http://pan.baidu.com/[redacted]

Xcode 6.0.1: http://pan.baidu.com[redacted]

Xcode6系列下载： http://pan.baidu.com[redacted]

4. Classification of iOS malware (XIII)

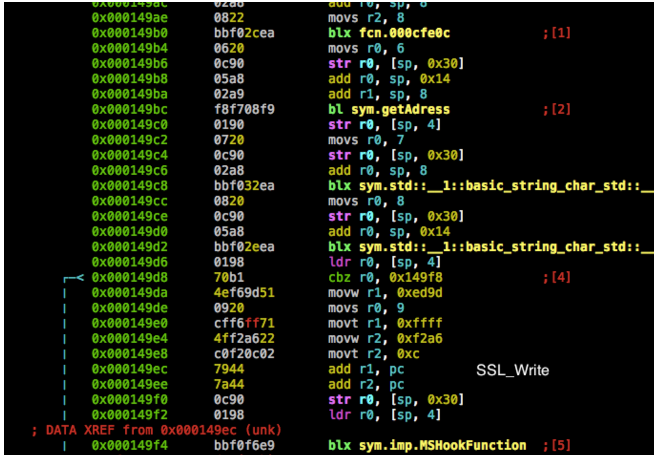
Attack vector

Attacking jailbroken devices

- **Cydia App & extensions (tweak)**
  - Cydia Apps can possess higher permission than StoreApps
    - Can access the whole filesystem
    - In most cases, Cydia Apps' install packages are .deb
    - Owner and (owner) group are usually root and admin
  - **Mobile Substrate framework**
    - Infrastructure of most tweaks
    - All the tweaks in Cydia work as dylibs
    - Placed in /Library/MobileSubstrate/DynamicLibraries
    - MSHookMessageEx and MSHookFunction

http://www.cydiasubstrate.com/api/c/

Most KeyRaider samples hook SSLRead and SSLWrite functions in the itunesstored process.

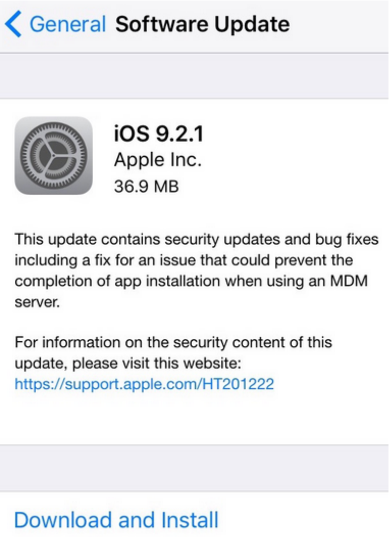


```
     0x000149ac    02a8        add r0, sp, 8
     0x000149ae    0822        movs r2, 8
     0x000149b0    bbf02cea    blx fcn.000cfe0c              ;[1]
     0x000149b4    0620        movs r0, 6
     0x000149b6    0c90        str r0, [sp, 0x30]
     0x000149b8    05a8        add r0, sp, 0x14
     0x000149ba    02a9        add r1, sp, 8
     0x000149bc    f8f708f9    bl sym.getAdress              ;[2]
     0x000149c0    0190        str r0, [sp, 4]
     0x000149c2    0720        movs r0, 7
     0x000149c4    0c90        str r0, [sp, 0x30]
     0x000149c6    02a8        add r0, sp, 8
     0x000149c8    bbf032ea    blx sym.std::__1::basic_string_char_std::_
     0x000149cc    0820        movs r0, 8
     0x000149ce    0c90        str r0, [sp, 0x30]
     0x000149d0    05a8        add r0, sp, 0x14
     0x000149d2    bbf02eea    blx sym.std::__1::basic_string_char_std::_
     0x000149d6    0198        ldr r0, [sp, 4]
  ┌─< 0x000149d8    70b1        cbz r0, 0x149f8               ;[4]
  |   0x000149da    4ef69d51    movw r1, 0xed9d
  |   0x000149de    0920        movs r0, 9
  |   0x000149e0    cff6ff71    movt r1, 0xffff
  |   0x000149e4    4ff2a622    movw r2, 0xf2a6
  |   0x000149e8    c0f20c02    movt r2, 0xc
  |   0x000149ec    7944        add r1, pc           SSL_Write
  |   0x000149ee    7a44        add r2, pc
  |   0x000149f0    0c90        str r0, [sp, 0x30]
  |   0x000149f2    0198        ldr r0, [sp, 4]
; DATA XREF from 0x000149ec (unk)
  |   0x000149f4    bbf0f6e9    blx sym.imp.MSHookFunction  ;[5]
```

5. Some Recommendations

5. Some recommendations (I)

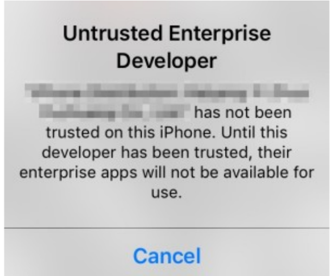
- **Update your applications and OS timely**
- Set a **passcode**
- Don't install applications from **unofficial/untrusted sources**.
- Don't allow using apps from **untrusted developer** *or* **untrusted enterprise developer**
- List of available trust root certificates in iOS 9 https://support.apple.com/en-us/HT205205



iOS 9.2.1
Apple Inc.
36.9 MB

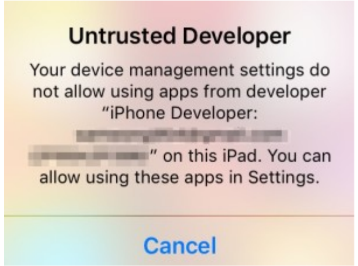
This update contains security updates and bug fixes including a fix for an issue that could prevent the completion of app installation when using an MDM server.

For information on the security content of this update, please visit this website:
https://support.apple.com/HT201222



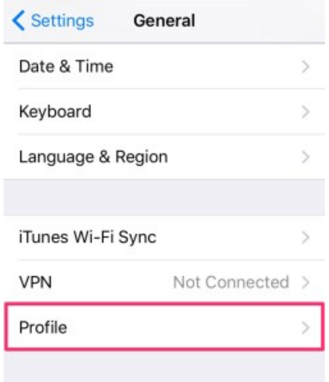
Untrusted Enterprise Developer

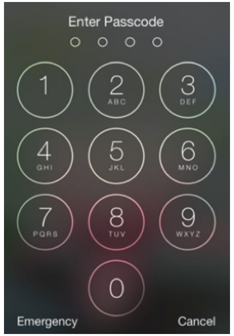
[redacted] has not been trusted on this iPhone. Until this developer has been trusted, their enterprise apps will not be available for use.



Untrusted Developer

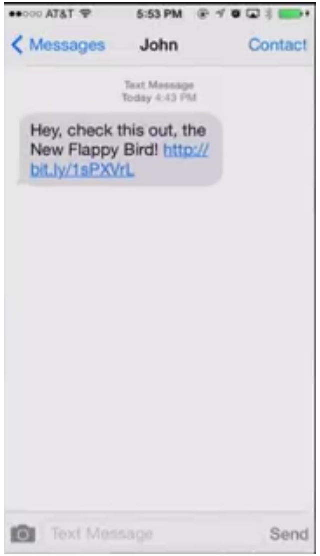
Your device management settings do not allow using apps from developer "iPhone Developer: [redacted]" on this iPad. You can allow using these apps in Settings.





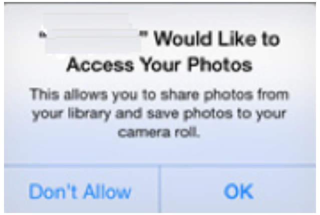
5. Some recommendations (II)

- Don’t click “Install” on a **pop-up** from a **third-party web page**.
- Don't trust in **unsolicited emails** or **SMS/MMS messages** suggesting smartphone applications need updating.
- Don't trust in pop-ups applications to gain access to **sensitive information** (contacts, photos, current location, calendar, etc). Click "OK" at your own risk.

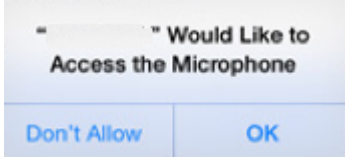


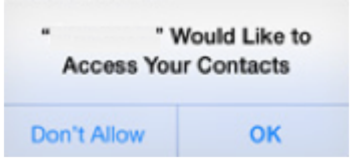
Text Message
Today 4:43 PM

Hey, check this out, the New Flappy Bird! http://bit.ly/1sPXVrL


"[redacted]" Would Like to Access Your Photos

This allows you to share photos from your library and save photos to your camera roll.


"[redacted]" Would Like to Access the Microphone


"[redacted]" Would Like to Access Your Contacts

5. Some recommendations (III)

- Download from the official **App Store**, or organization’s internal applications under your IT department’s guidance.
- Even applications from the App Store can also **abuse private APIs** for harmful operations.
- Beware of plug-in iOS devices on a compromised laptop via USB cable.

Download on the App Store

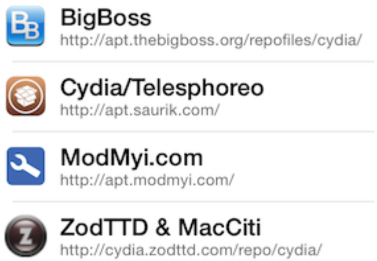
Can Apple Keep App Store Malware Free?

5. Some recommendations (IV)

- Don’t **jailbreak** mobile phones
- Use all Cydia repositories **at your own risk**
  - Evaluate the **reputation** of the package and the developer
  - Evaluate how the package is **distributed**
    - Via default repositories
    - Repositories hosting pirated packages
    - Distributing tweaks without developer permission

https://www.reddit.com/r/jailbreak/wiki/howtoresearch

/r/Jailbreak
tweaks, news, and more for jailbroken iPhones, iPads, and iPod touches.


BigBoss
http://apt.thebigboss.org/repofiles/cydia/

Cydia/Telesphoreo
http://apt.saurik.com/

ModMyi.com
http://apt.modmyi.com/

ZodTTD & MacCiti
http://cydia.zodttd.com/repo/cydia/

6. Related work

6. Related Work: on Android malware

- Reference behaviour, analysis approach, malware behaviour (Amamra et al., MALWARE'12)
- Current and future incentives (Felt et al., SPSM'11)
  - 46 samples analyzed, 4 of them were iOS malware
- Attack type and installation methods (Zhou & Jiang, S&P'12)
  - 1200 samples analyzed
- ANDRUBIS (Lindorfer et al., BADGERS'14)
  - Dynamic analysis tool
- Attack goals, malware behaviour, distribution, infection, and privilege acquisition (Suárez-Tangil et al., Comm. Surv. 2014)
  - Really nice survey. 9 samples belong to iOS

6. Related Work: on iOS tools

- PiOS (Egele et al., NDSS'11)
  - Static analysis; detect exfiltration of sensitive information
- XiOS (Bucicoiu et al., ASIA-CCS'15)
  - Mitigate attacks as lazy bindings or abuse of private APIs
- iRiS (Deng et al., CCS'15)
  - Better vetting system
  - Static and dynamic analysis
- Abuse of iOS sandboxing (Xing et al., CCS'15)
  - Inter-app interaction services

7. Conclusions & Future work

7. Conclusions & future work (I)

- Mobile malware are rapidly emerging
- iOS security strongly relies on vetting process
  - Still fruitless, several ways to bypass it

- Few samples target at non-jailbroken devices
- Few samples exploit iOS vulns
- Data theft and spying are common goals

7. Conclusions & future work (II)

- In the future, we expect:
  - More samples targeting at non-jailbroken devices
  - A diversity of attack goals

- Future work
  - Find binary similarities among samples (malware clustering)
  - Identify data to build useful IOCs (e.g., stolen certificates)

- MLW.RE
  - For providing us with samples <3
- Radare2 community
  - For maintaining r2 for free ^.^
- The iPhone Wiki
- RootedCON

Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
return