ignite 2015

LAS VEGAS | THE COSMOPOLITAN | MARCH 30–APRIL 1, 2015

iOS Malware

New Techniques, Trends, and Ecosystems

Claud Xiao
Palo Alto Networks

Outline

WireLurker → Malware → Trends → Ecosystem → Insecure

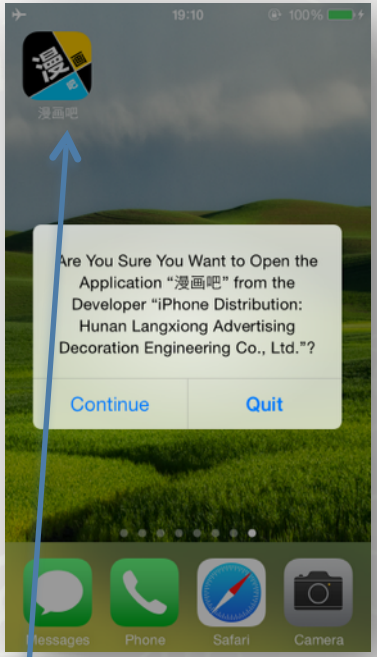
WireLurker: Why It's Serious?

A New Era of iOS Malware

The first in-the-wild malware that

- automatically attacks iOS through OSX/Windows via USB
- automatically generates malicious iOS app
- infects installed iOS apps
- targets non-jailbroken iOS devices


app.maiyadi.com/app-675041/#p=1
苹果论坛快速入口
麦芽地
APP STORE
APP 搜索
APP STORE
iPhone软件
iPad软件
Mac软件
CleanApp (Mac)
一句话点评
苹果软件卸载工具
3090 人下载
Mac OS X
暂无一键安装
免费版下载


Are You Sure You Want to Open the Application "漫画吧" from the Developer "iPhone Distribution: Hunan Langxiong Advertising Decoration Engineering Co., Ltd."?
Continue
Quit

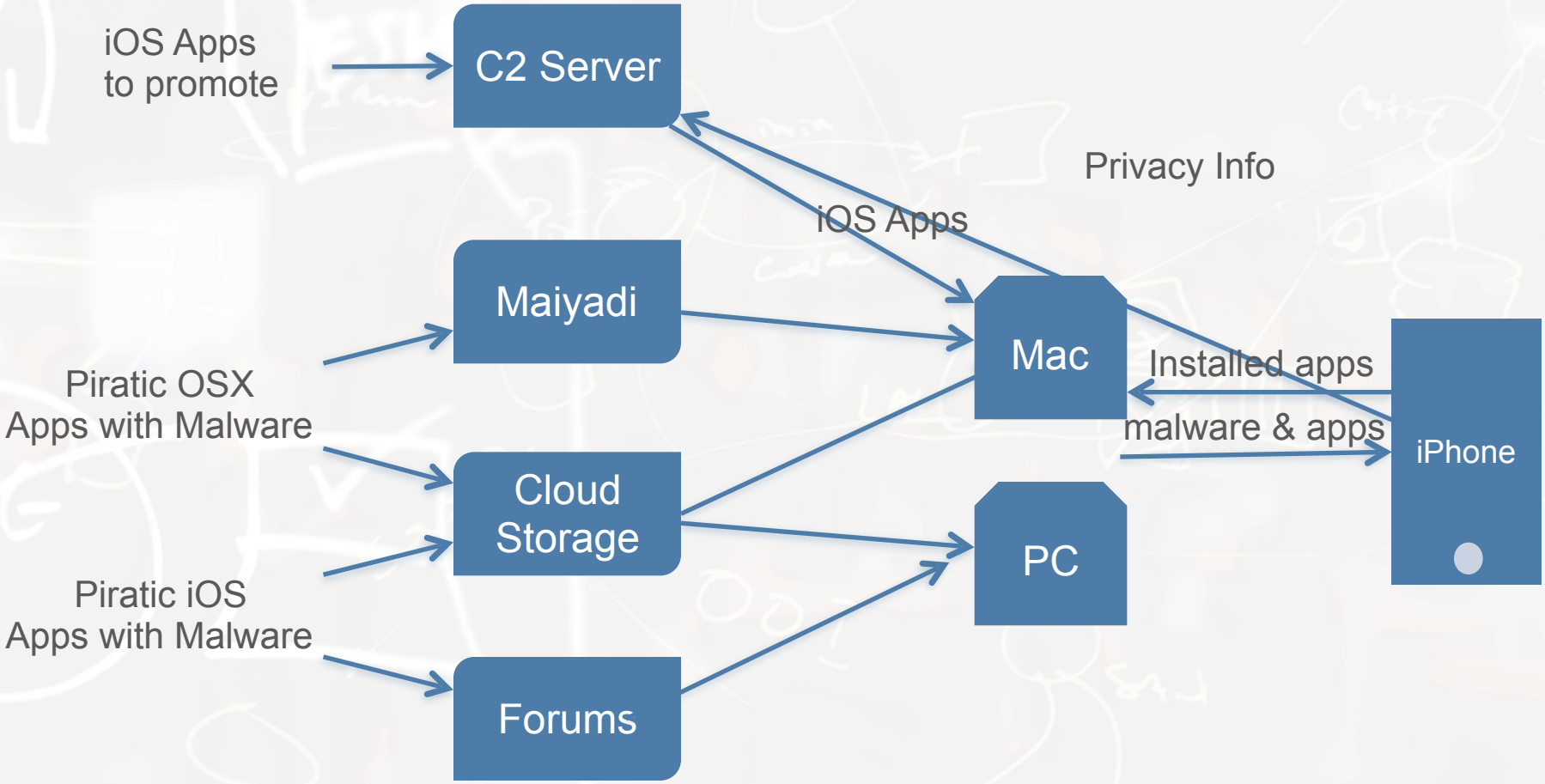

dl.vmall.com/c0nu5dwv4m
外链资源库
CleanApp 4.0.8 Mac 中文版.dmg
下载
转存网盘


CleanApp 4.0.8 Mac 中文版
CleanApp.app
CORE Keygen.app
QQ 381857416


ekangwen206
+ 立即订阅
Ta还没有个人说明呢
自由存，随心享
245分享 0专辑 0订阅 64粉丝
全部分享 专辑 图片 文档 音乐 视频 其他
分享文件 分享时间 浏览次数 保存次数 下载次数
讯飞语音输入 1.0.1073.rar 2014-03-13 21:16 254次 20次 179次
音悦台 1.2.5.7.rar 2014-03-13 21:16 270次 17次 194次
鳄鱼小顽皮爱洗澡 1.13.0.rar 2014-03-13 21:16 78次 13次 43次
龙珠祖玛 1.9.0.rar 2014-03-13 21:16 88次 12次 47次
OPlayer 2.0.12.rar 2014-03-13 21:15 74次 11次 49次


绿色IPA安装器
WhatsApp
软件版本： 2.11.7
软件大小： 14.20M
软件标示： net.whatsapp.WhatsApp
固件需求： IOS4.3及以上
请先安装ITunes
连接设备

Attacking Vector



Infections

- Was embedded into 534 Mac apps, 180 Windows software
- 421,317 downloads (84.5% for Mac)
- After we released detection tool, lot of victims feedback infections


```
python WireLurkerDetectorOSX.py
WireLurker Detector (version 1.0.0)
Copyright (c) 2014, Palo Alto Networks, Inc.

[+] Scanning for known malicious files ...
[!] Found malicious file: /Library/LaunchDaemons/com.apple.machook_damon.plist
[!] Found malicious file: /usr/bin/WatchProc
[!] Found malicious file: /usr/bin/itunesupdate
[!] Found malicious file: /Library/LaunchDaemons/com.apple.watchproc.plist
[!] Found malicious file: /Library/LaunchDaemons/com.apple.itunesupdate.plist
[!] Found malicious file: /System/Library/LaunchDaemons/com.apple.appstore.plughelper.plist
[!] Found malicious file: /System/Library/LaunchDaemons/com.apple.MailServiceAgentHelper.plist
[!] Found malicious file: /System/Library/LaunchDaemons/com.apple.systemkeychain-helper.plist
[!] Found malicious file: /System/Library/LaunchDaemons/com.apple.periodic-dd-mm-yy.plist
[!] Found malicious file: /usr/bin/com.apple.MailServiceAgentHelper
[!] Found malicious file: /usr/bin/com.apple.appstore.PluginHelper
[!] Found malicious file: /usr/bin/periodicdate
[!] Found malicious file: /usr/bin/systemkeychain-helper
[!] Found malicious file: /usr/bin/stty5.11.pl
[+] Scanning for known suspicious files ...
[!] Found suspicious file: /etc/manpath.d/
[+] Scanning for infected applications ... (may take minutes)
[-] Nothing is found.
[!] WARNING: Your OS X system is highly suspicious of being infected by the WireLurker.
[!] You may need to delete all malicious or suspicious files and/or applications above.
```

Attacking Methods

- Application repackaging on Mac OS X and iOS
  - Simply binary replacement
  - Looks like but simpler than virus infection
  - Compare with Android app repackaging
- Windows installers are also automatically generated

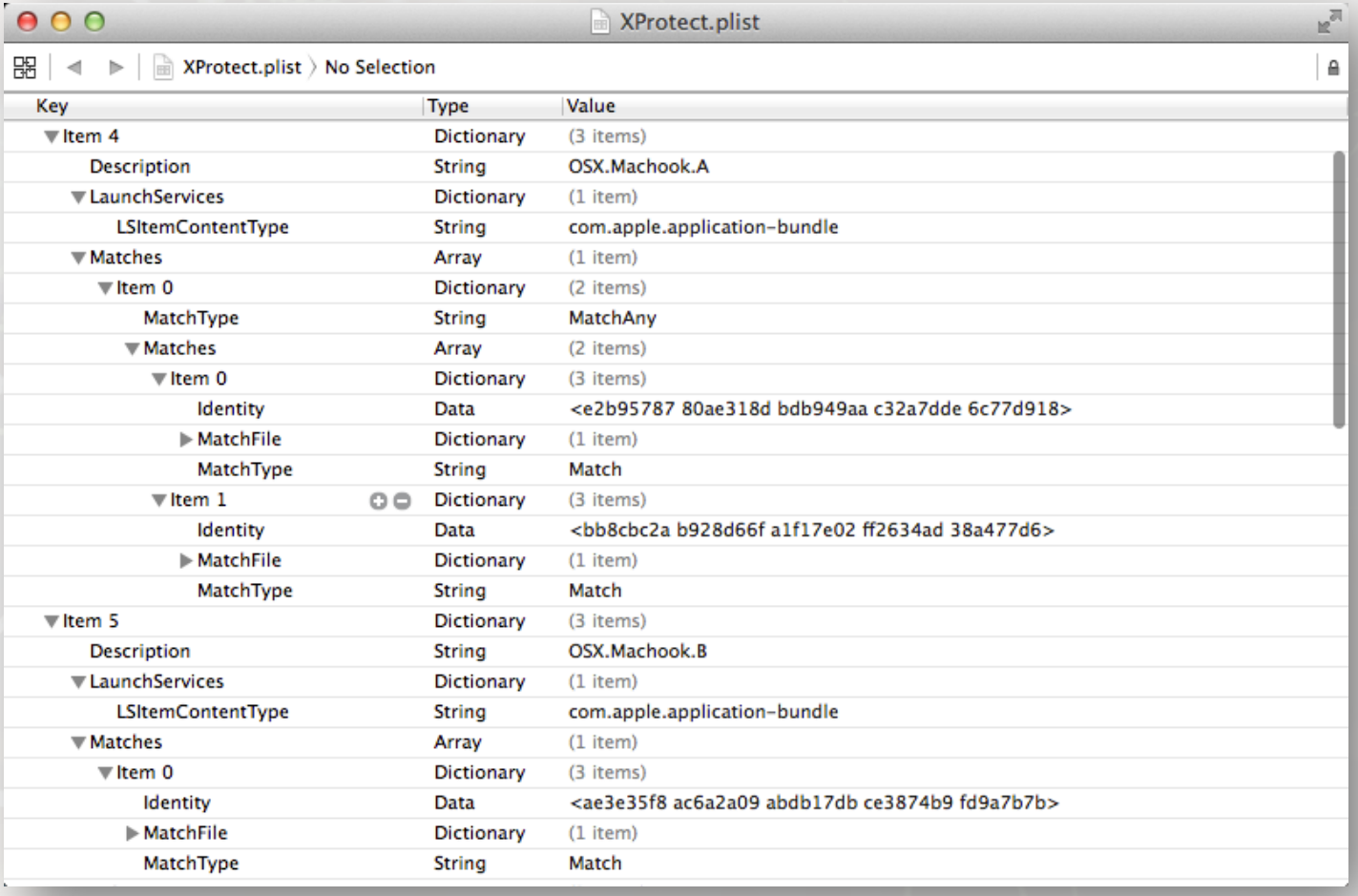

```
BadPiggies.app/
  Contents/
    Info.plist
    MacOS/
      Bad Piggies
      Bad Piggies_
```

Attacking Methods (cont.)

- Install apps through USB by iTunes protocol
  - Classic method of using the `libimobiledevice`
  - Just like what *Matcans* and *Mekir* did
- Infect installed iOS apps
- Abusing Cydia Substrate framework
  - Pretty popular in previous iOS spyware and malware
- In-house iOS app distribution
  - Abusing Apple's enterprise program
  - Has been abused in a long time in China
- The Masque attack ?

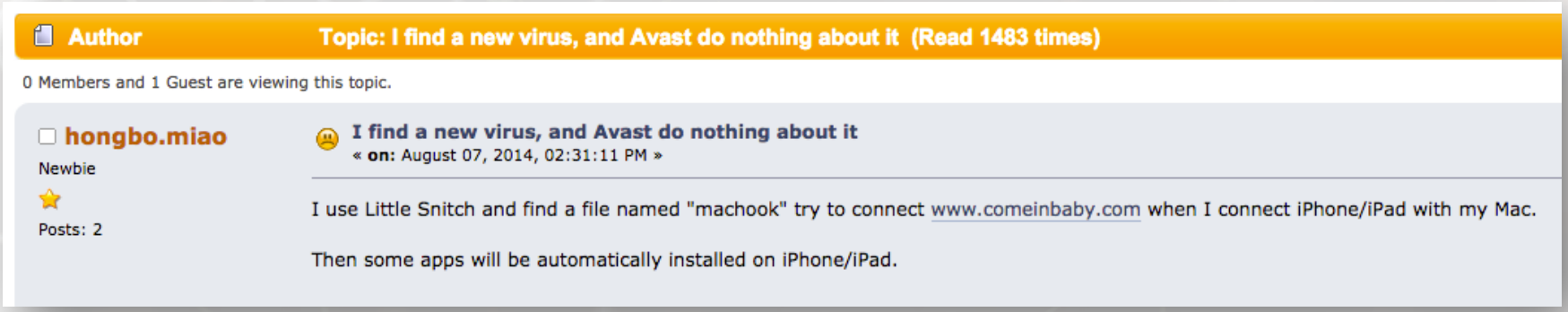
Updates (cont.)

- Apple updated Xprotect signatures twice to prevent it
  - But victims were not well protected due to its signatures and protection model



Updates (cont.)

- Other countries were also affected (from Kaspersky's blog)
  - Canada
  - France
  - UK
  - US
  - Korea
- The sample was reported to security companies before we published the report



Author | Topic: I find a new virus, and Avast do nothing about it (Read 1483 times)

0 Members and 1 Guest are viewing this topic.

hongbo.miao
Newbie
Posts: 2

I find a new virus, and Avast do nothing about it
« on: August 07, 2014, 02:31:11 PM »

I use Little Snitch and find a file named "machook" try to connect www.comeinbaby.com when I connect iPhone/iPad with my Mac.

Then some apps will be automatically installed on iPhone/iPad.

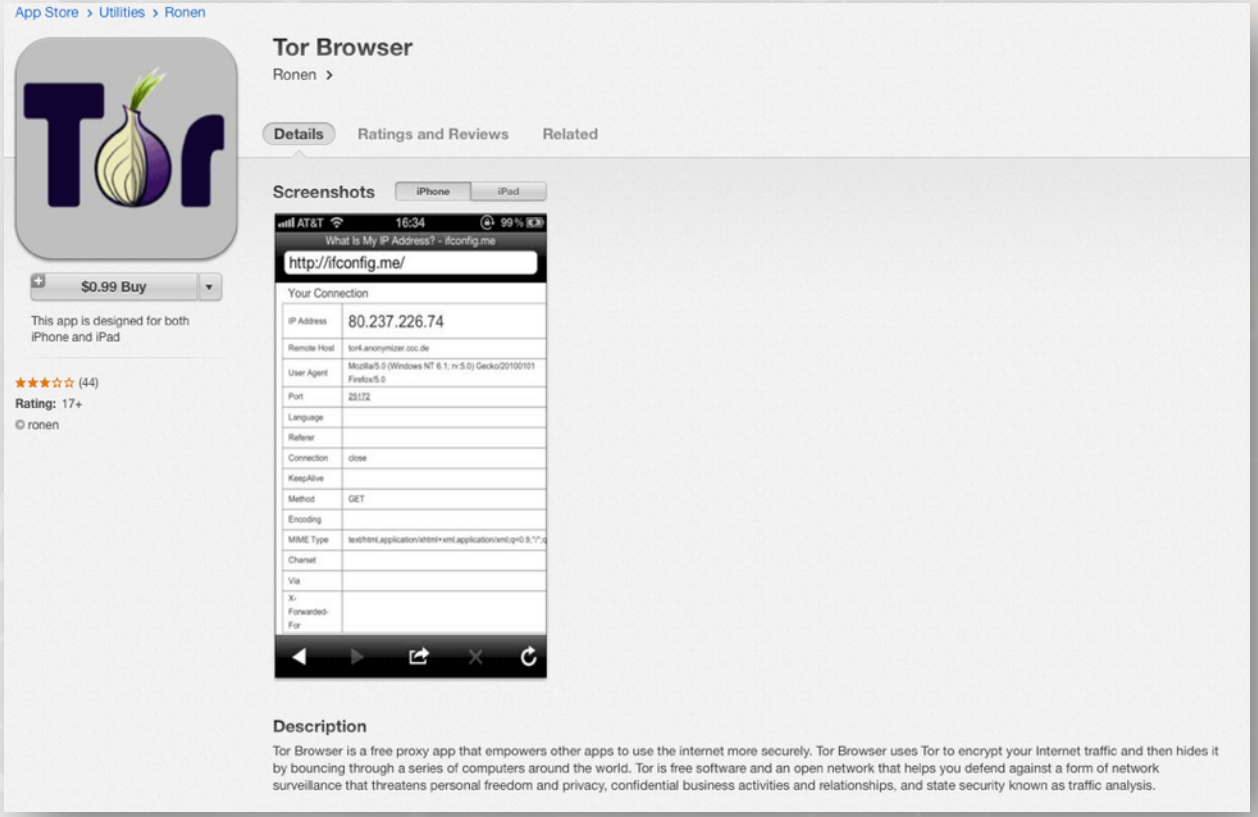
Updates

- 3 suspects were arrested in Beijing
  - Only after a week of our report
  - They’re managers and developer of the Maiyadi
  - The C2 server and the Maiyadi were closed
  - http://www.theregister.co.uk/2014/11/17/wirelurker_suspects_china_arrests/

Other iOS Malware in 2014

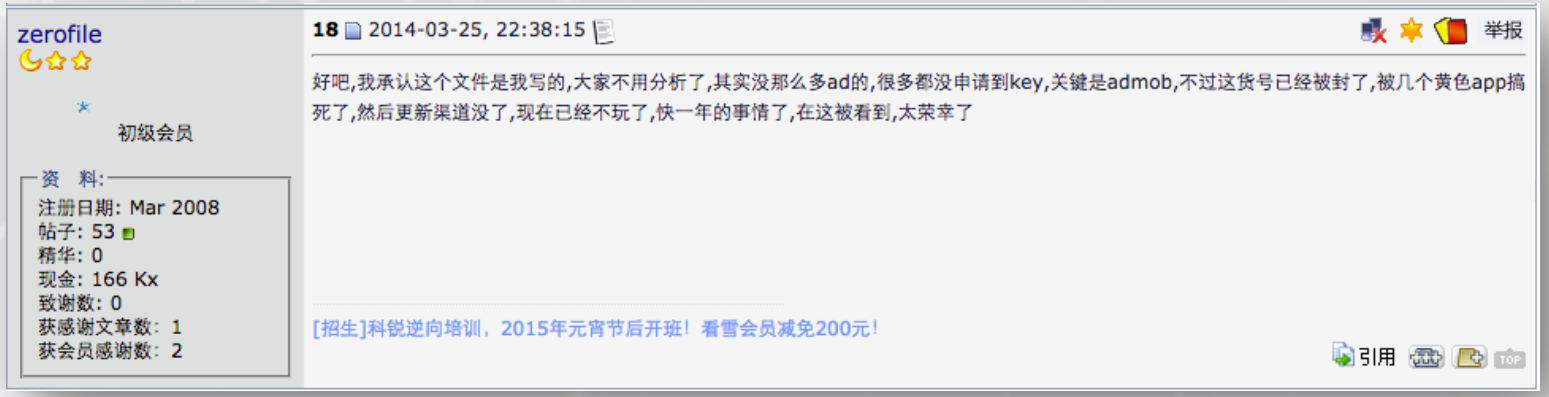
FakeTor, Adware in App Store

- Not affiliated with the Tor Project
- “It’s full of adware and spyware.” by a high-ranking Toe volunteer



AdThief, Steals Advertisement Revenue

- Replace developer ID of 15 advertisement libraries in other apps to steal promotion fee from app developers
- Statistics from one of targeted ad service providers:
  - Infected devices: ~75,000
  - All ad requests: ~22 millions
  - Daily ad requests: ~20,000
- Hey, author's here:



Unflod, Steals Apple ID and Password

- By using Cydia Substrate on jailbroken devices,
- hook the `SSLWrite`, hijack SSL traffic in iTunes service's authentication session, steal Apple ID and password(!) in it
  - Super easy to implement

```
if ( !findhead )
{
  v19 = strstr(v22, auth);                    // /WebObjects/MZFinance.woa/wa/authenticate HTTP/1.1
  if ( v19 )
  {
    findhead = 1;
    strcpy(content, v22);
  }
}
if ( findhead == 1 )
{
  v18 = strstr(v22, appleId);                 // <key>appleId</key>
  v17 = strstr(v22, password);                // <key>password</key>
  if ( v18 )
  {
    if ( v17 )
    {
      strcat(content, v22);
      v16 = strstr(content, "</plist>");
      if ( v16 && v16 - content <= 2040 )
        v16[8] = 0;
```

AppBuyer, Buy Apps on Your Behalf

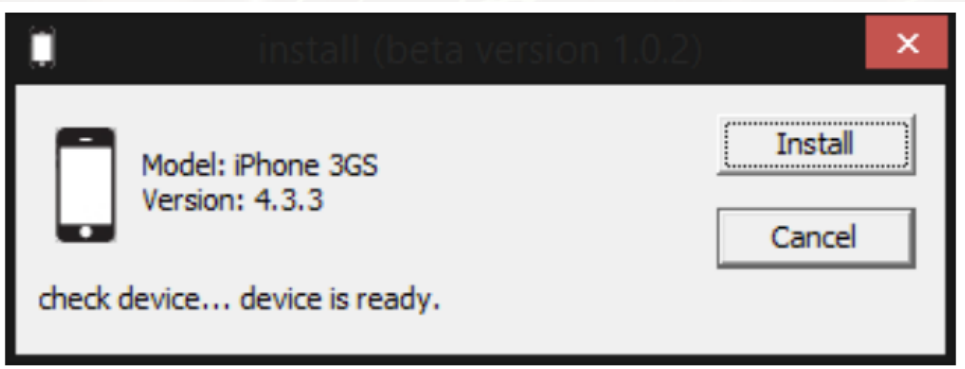
- Steal Apple ID and password by the same method Unflod used
- Construct iTunes communications to purchase apps by your Apple ID and download/install them to your iDevices

```
__strcpy_chk(
  &xml,
  "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\n<!DOCTYPE plist PUBLIC \"-//Apple//DTD PLIST
  10240);
errcode = 0;
replacestr(&xml, "[AID]", v30);
replacestr(&xml, "[AID]", v30);
replacestr(&xml, "[GUID]", &guid);
replacestr(&xml, "[KBSYNC]", &kbsync);
__sprintf_chk(&v32, 0, 1024, "%d", isfee);
replacestr(&xml, "[PRICE]", &v32);
__sprintf_chk(&v35, 0, 256, "p%d-buy.itunes.apple.com", serverno);
__sprintf_chk(&v34, 0, 1024, "/WebObjects/MZBuy.woa/wa/buyProduct");
v24 = gethostbyname((const char *)&v35);
if ( v24 )
{
  v27 = socket(2, 1, 0);
```

- Remote code downloading and execution
- Remotely controlled

Mekir, Spreads Through PC

- Found by Kaspersky, iOS part of samples is not public available yet
- Infect Android, (jailbroken) iOS, Windows Mobile and Blackberry from Windows and OS X
- iOSInfector has an user interface



Main window of the iOS infector

From: http://press.kaspersky.com/klcsd/files/2014/06/Blogpost_KL_HackingTeam2_Final.pdf

Xsser, Collects Privacy of Specific People

- Target the “Occupy Central” protests in Hong Kong
- Collects and uploads information
  - Contacts
  - SMS
  - Call logs
  - Location
  - Photos
  - Tencent Wechat log
  - Apple Keychain data

Cloudatlas in APT

- Used in the Red October APT operation
- Spread through Email phishing
  - `WhatsAppUpdate.deb`
- Android, iOS and Blackberry versions
- Collect devices info and user info

```
DEVICE PLATFORM: '%@'\n
DEVICE NAME: '%@'\n
DEVICE LOCALIXES MODEL: '%@'\n
DEVICE MODEL: '%@'\n
DEVICE SYSTEM NAME: '%@'\n
DEVICE SYSTEM VERSION: '%@'\n
ICCID: '%@'\n
InternationalRoamingEDGE: '%@'\n
InternationalRoamingEDGE
Phone number: '%@'\n
PhoneNumber
CarrierBundleName: '%@'\n
CarrierBundleName
ISO CONUTRY NAME: '%@'\n
CARRIER NAME: '%@'\n
MCC: '%@'\n
MNC: '%@'\n
STATE CONNECTION: 'WiFi'\n
MAC ADDRESS: '%@'\n
DEVICE BATTERY LEVEL: '%f'\n
FREE SPACE: '%f GB'\n
TOTAL SPACE: '%f GB'\n
CPU FREQUENCY: '%lu'\n
CPU COUNT: '%lu'\n
TOTAL MEMORY: '%lu' Mb\n
USER MEMORY: '%lu' Mb\n
```

What's New in the Past Year

Keywords

Jailbreak

Cydia Substrate

USB, Cross platform infection

APT, targeted

Apple ID

App/Ad promotion

Cross platform available

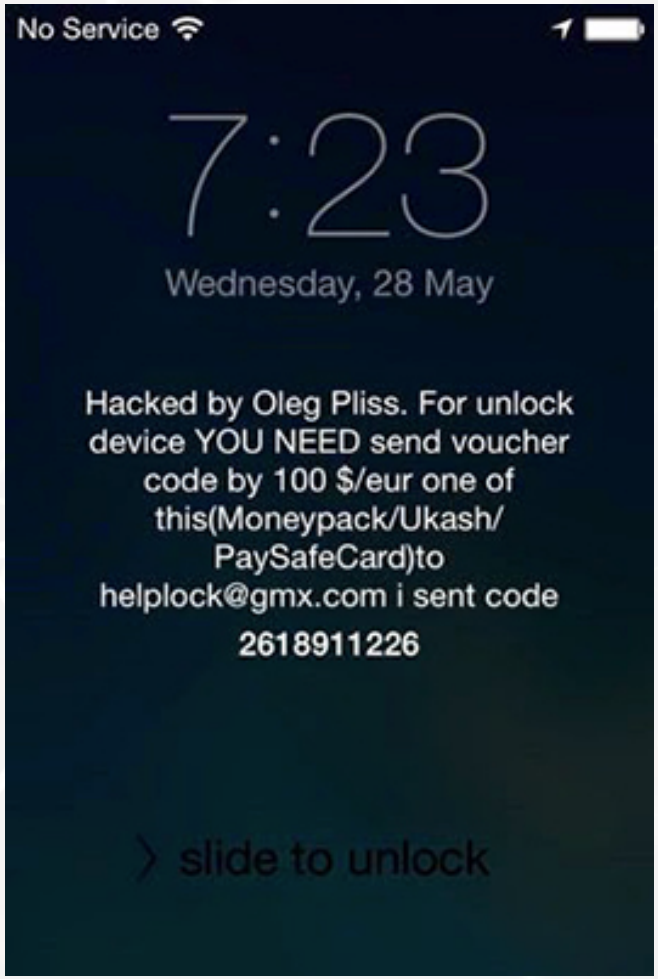
Spreading and Attacking

- Targeted attacking, phishing, combination with APT operation
  - *Xsser*: WhatsApp message phishing
  - *Cloudaltas*: Email phishing
- Cydia sources
  - Most of iOS commercial Spyware are hosting on 3rd party Cydia repository
  - Physically access or cheating is needed to infect
- Mac/PC -> USB -> iDevices
  - Solved the automatically infection problem
- Enterprise distribution program
  - Solved the jailbreaking problem
- More on the Masque attack

Profit Making

- In-device app promotion
- Apple account for app promotion
- Apple ID for SMS spam
- Apple account for Ransom
- Apple account for data stealing
- Advertisement
- Politic purpose

Ransom by Stolen Apple Account



Challenges to Automatically Analysis

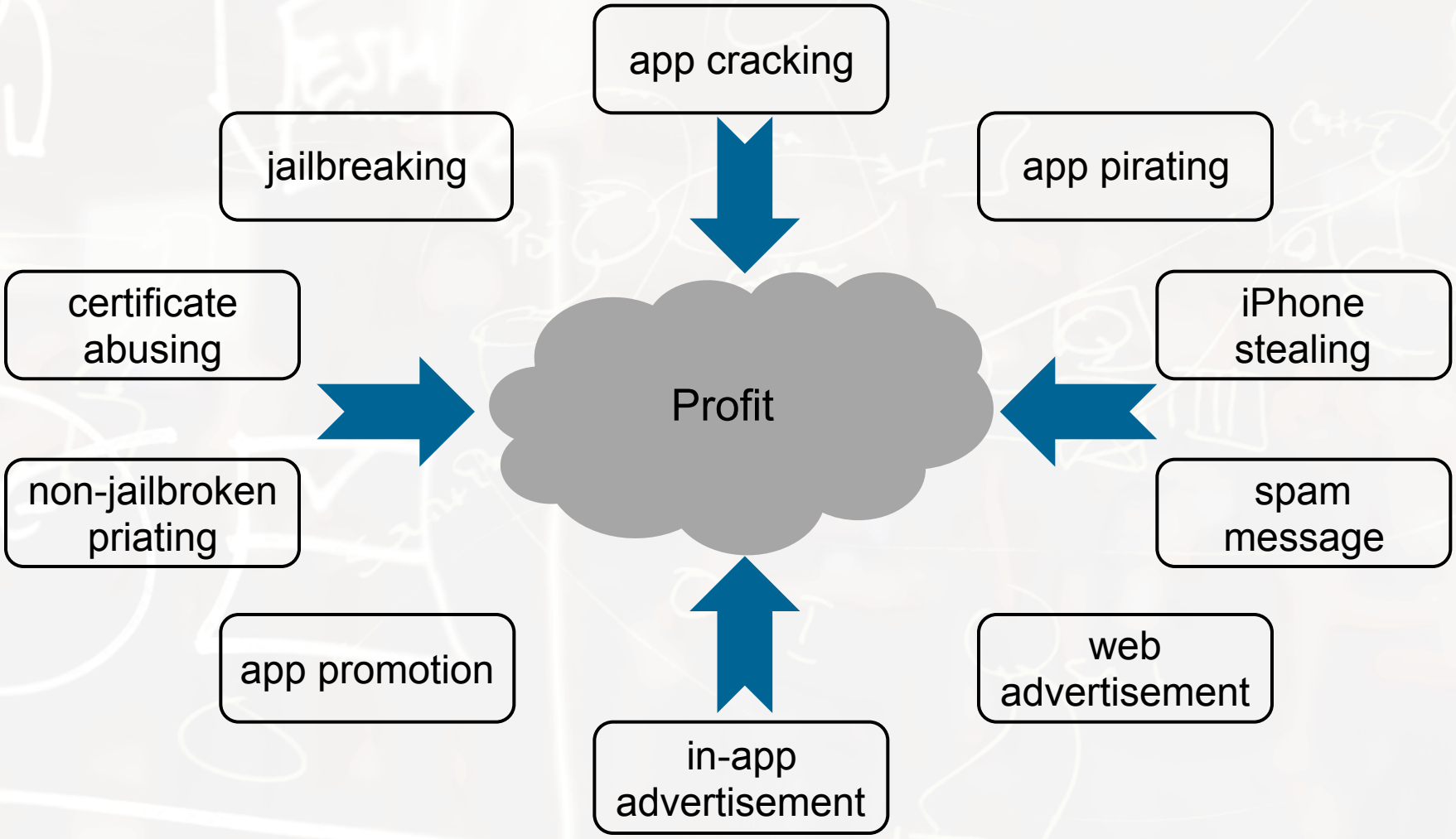
- Harder to find samples: they're targeted or small range spread
- Samples' formats: DEB package or Mach-O + Plist
- Runtime: Jailbroken + Cydia Substrate
- Lots of behaviors are out of sandbox
  - How to monitor?
  - How to restore system?

Gray Area of iOS Ecosystem in China

Questions

- Many iOS malware come from or target China. Why?
- Is jailbroken device a considerable attacking target?
- What do them collect Apple ID and password for?
- Why they purchase iOS apps in infected devices?
- How could users be infected?

All for Profit, and All Can Make Profit Directly



Jailbreaking as a Business

- Providing jailbreak tool
- Providing online or offline jailbreak service

iCloud Account Phishing

关于您遗失的iPhone信息 ☆

发件人: Apple信息 <icloud@apple.com>
(由 appkeyid@china.com 代发)
时 间: 2014年7月30日(星期三) 凌晨0:27
收件人: 绿云逸 <307743733@qq.com>

这是一封垃圾箱中的邮件。请勿轻信中奖、汇款等虚假信息，勿轻易拨打陌生电话。 举报垃圾邮件 移回收件箱

尊敬的苹果用户：您好！

您的Apple ID被多次尝试激活一台可能为丢失模式的"iphone"设备。如果不是您本人操作的，请立即前往官网验证您的信息，以便我们对该账户异常情况进行处理，如果验证成功，我们将为您远程锁定该设备，阻止其激活使用，并将尝试激活该设备的手机号码及IP地址以邮件的形式发送至您的邮箱，以便协助您找回丢失的设备。

时间: 2014年7月28日.设备系统: iphone ios,7.1.2,11B554a

立即验证

如果您未丢失此设备，请忽略此封电子邮件。
为了能够及时的反馈您的信息，请务必填写正确的Apple ID邮箱格式及密码，如果您忘记了您的Apple ID密码，您可以前往 iforgot.apple.com重设您的密码。

谨上
Apple 客户服务

“Well, why should I care about what happens in China?”

Impacts to Other Countries

- Attacking techniques and ideas' improvement and spreading
- Global developers or VIPs may be under attack
- Global normal users are also affected

Earliest Enterprise Certificate Abusing

GBA4iOS 1.6.2

- Supports iOS 6
- Compatible with classic GBA4iOS Save States
- Original GBA4iOS skins

IMPORTANT: *Before* downloading, open Settings > General > Date & Time, and set the date back *at least* one day in the past. Once GBA4iOS has downloaded, open it, then set the date back to normal. If GBA4iOS fails to open again later, set the date back, open GBA4iOS, and then set the date back to normal.


Rethink iOS Security

Jailbroken iOS Devices

- Cydia package manager
  - Directly provides highest privilege to all 3rd party packages
  - Hides packages' dependency relationship from users
- Cydia Substrate and its tweaks
  - Provides interfaces for tweaks to easily hook other iOS apps
  - Not notify users nor ask for their confirmation
- Cydia repositories
  - Easily create and maintain any 3rd party repositories
  - Most repositories haven't any app review mechanism

Non-jailbroken iOS Devices

- Enterprise Program
  - A way to install apps from USB or 3rd party website
  - A way to bypass Apple's code reviewing
  - A way to use non-public APIs
  - A way to open the first door in jailbreaking
- Trust relationship to Mac/PC
  - Commands from Mac/PC != Commands made by the owner
- And lots of vulnerabilities
  - e.g., URL scheme hijacking

Conclusions

Thank you for your time!

Thanks to Chao Qu, CDSQ, cryptax,

Royce Lu, Rob Downs, Zhi Xu, Hui Gao and Ryan Olson