

Art of Dancing with Shackles

- Best Practice of App Store Malware Automatic Hunting System

- Ju Zhu, @ju__zhu
- Lilang Wu, @Lilang_Wu
- Moony Li, @Flyic

What We Will Cover

- Who We Are
- Auto Sample Crawl System
- Sandbox Analysis System
- Demo

A glowing orange waveform, resembling a sound wave or a stylized heartbeat, is centered horizontally across the image. The waveform has multiple peaks and valleys, with the central peak being the most prominent. The background is solid black, which makes the bright orange line stand out. The text "Who We Are" is superimposed on the waveform, centered between the peaks.

Who We Are



Moony Li

- @Flyic
- 8 years security
- Sandcastle
- Deep Discovery
- Exploit Detection
- Mac/Windows Kernel
- iOS/Android Vulnerability



Ju Zhu

- @ju__zhu
- 5+ years mobile security
- Mobile Advanced Threat Research
- Hunt Mobile 0Day/nDay
- Mobile Vulnerability

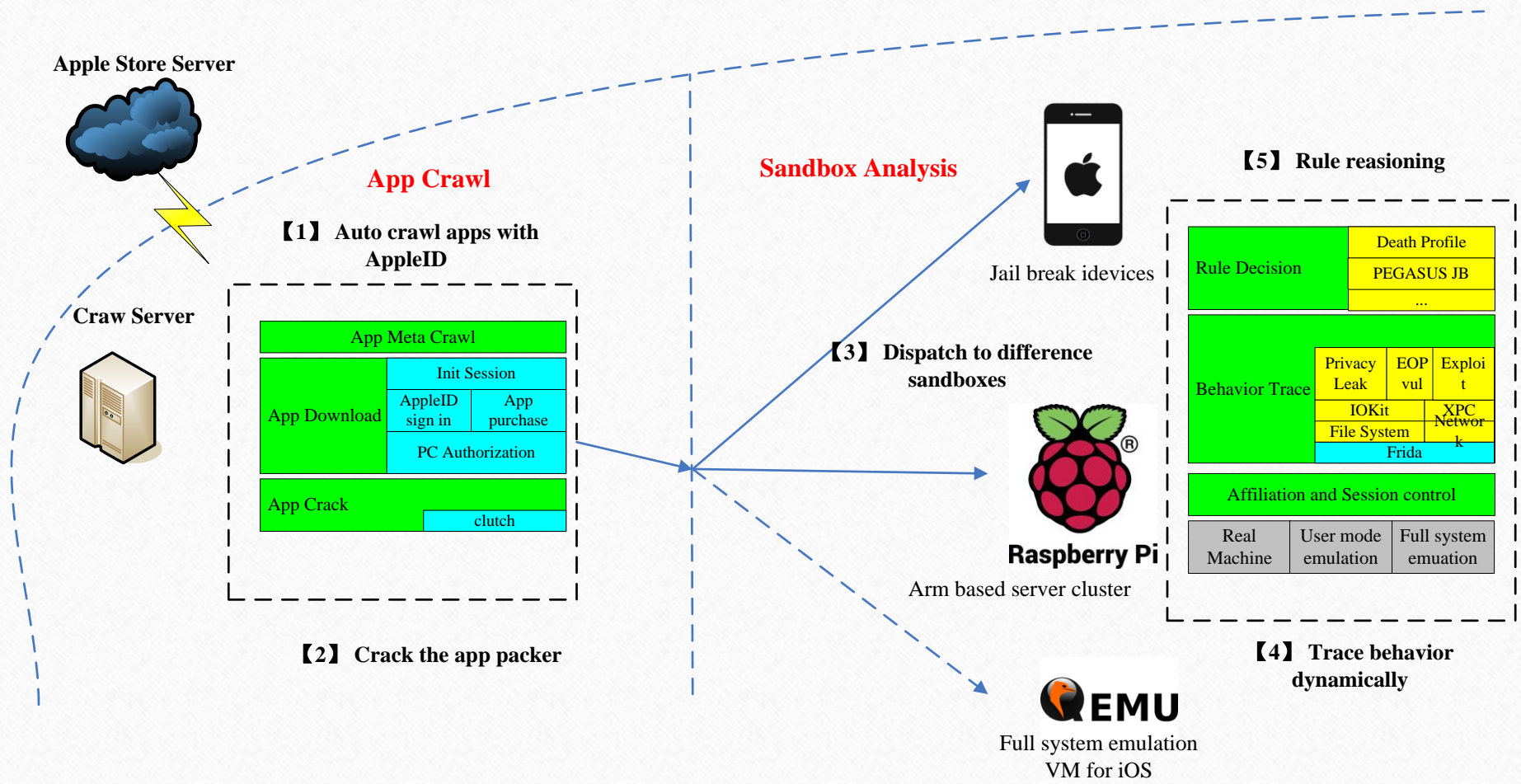


Lilang Wu

- @Lilang_Wu
- 3 years security
- Mobile Advanced Threat Research of TrendMicro
- Mac/iOS Vulnerability/Malware



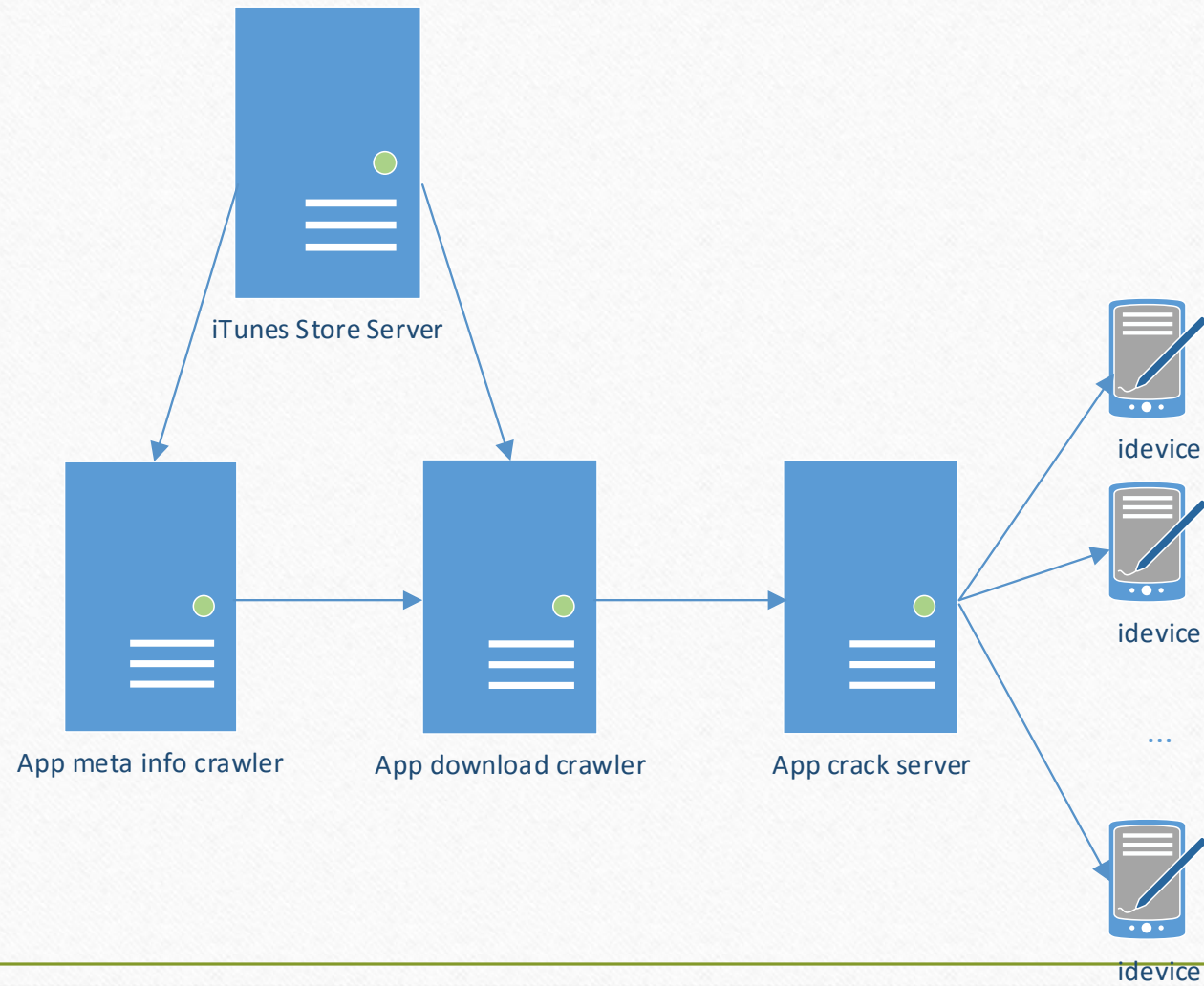
Automatic Malware Hunting System



Automatic Malware Hunting System

-Auto Crawl System

Overview



AppleStore malware hunting

ipa crawl

PC itunes

1. Sign in

guid an...

Requires

account

appleID
passwd

guid (on PC)

Mac address
System disk serial number
Productid
CPU info
MainBoard info
Computer Name
Profile tail

generate

passwordToken
dsPersonId

2. Buy product

Sign in

Requires

account

appleID
passwd

guid (on PC)

appid

sign in info

passwordToken
dsPersonId

generate

IPA file without sinf

NO sinf

3. Online operation

Sign in

Rate

Require

Sign in
appid
guid (on PC)

Star(from you)

Review

Require

Sign in
appid
guid (on PC)

Start(from you)

title (from you)

body(from you)

Search keywords

require

sign in
keyword (from you)

generate

app_ids
app_infos

4. install

Requires

IPA file

udid

appleID

IPA

5. run

Requires

Binding Apple...

sinf file

appleID

IPA file

???guid (on PC)

TimeStamp

Avoid appleID popup

Sign in device with appleID once

Patch appleID check

IPA Crack

Clutch

Emulate exec???

Behavior Sandbox

IPA install and run

Frida trace

decision engine

Key Points



Auto Crawler System

- App Meta info Crawler

01

- App Download Crawler

- initialize
- Apple ID sign in
- App purchase
- Sign the APPs

02

- App Crack Server

- iOS device Authorization
- PC Authorization

03

- Best practice

- for Anti-Anti Crawl
- for Apple ID Activation

04

Key Points



Auto Crawler System

• App Meta info Crawler

01

• App Download Crawler

- initialize
- Apple ID sign in
- App purchase
- Sign the APPs

02

• App Crack Server

- iOS device Authorization
- PC Authorization

03

• Best practice

- for Anti-Anti Crawl
- for Apple ID Activation

04

App Meta Info Crawler

- crawler based on Scrapy Crawling Framework
- different spiders for different region of iTunes Store

Key Points



Auto Crawler System

• App Meta info Crawler

01

• App Download Crawler

- initialize
- Apple ID sign in
- App purchase
- Sign the APPs

02

• App Crack Server

- iOS device Authorization
- PC Authorization

03




• Best practice

- for Anti-Anti Crawl
- for Apple ID Activation









04

App Download Crawler

- Four Steps:
 - Init Session and Keybag
 - Apple ID Sign In

☆ + 5.625	!	0.016 s	GET	200	3.18 K		https://init.itunes.apple.com/WebObjects/MZInit.woa/wa/signSapSetupCert
☆ + 5.641	!	0.812 s	POST	200	1.94 K		https://play.itunes.apple.com/WebObjects/MZPlay.woa/wa/signSapSetup
☆ + 6.469	!	0.562 s	POST	200	1.25 K		https://p18-buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/authenticate

- App purchase process

☆ + 7.031	!	0.360 s	GET	200	122.37 K		https://init.itunes.apple.com/bag.xml?ix=5&dsid=25176736755&sign-bsn=2
☆ + 7.469	!	1.062 s	GET	200	346		https://xp.apple.com/register
☆ + 8.531	!	0.813 s	POST	200	301		https://upp.itunes.apple.com/WebObjects/MZBookkeeper.woa/wa/getAll
☆ + 9.344	!	1.328 s	GET	200	64.64 K		https://itunes.apple.com/us/app/appname/id1224851236?mt=8
☆ + 10.672	!	0.984 s	POST	200	1.25 K		https://p18-buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/authenticate
☆ + 11.656	!	0.641 s	POST	200	18.46 K		https://p18-buy.itunes.apple.com/WebObjects/MZBuy.woa/wa/buyProduct
☆ + 12.344	!	30.922 s	GET	200	21.77 M		http://iosapps.itunes.apple.com/apple-assets-us-std-000001/Purple118/v4/3a/c8/22/3ac8221e-6a5a-6025-9982-657ea9b22cbd/
☆ + 43.781	!	0.219 s	GET	200	228		https://p18-buy.itunes.apple.com/WebObjects/MZFastFinance.woa/wa/songDownloadDone?Pod=18&songId=1224851236&guid=

- Sign the APPs

Key Points



Auto Crawler System

• App Meta info Crawler

01

• App Download Crawler

02

- initialize
- Apple ID sign in
- App purchase
- Sign the APPs

• App Crack Server

03

- iOS device Authorization
- PC Authorization

• Best practice

04

- for Anti-Anti Crawl
- for Apple ID Activation

App Download Crawler – Initialize

- Requirement to init Session ID
 - Cert key: calculated by system propertyies
 - $\text{session_id} = \text{plock}[0x24 / 4]$
- Requirement to init Keybag
 - Cert key: calculated by system propertyies
 - SC Info: iTunes authorization data file

```
.text:1022CEC6      push    offset RootPathName ; "C:\\\"
.text:1022CECB      call    ds:GetVolumeInformationW
.text:1022CED1      test    eax, eax
.text:1022CED3      jz      loc_1022D135
.text:1022CED9      push    4
.text:1022CEDB      lea     ecx, [ebp+VolumeSerialNumber]
.text:1022CEDE      jmp     loc_1022D129
.text:1022CEE3      ; -----
.text:1022CEE3      ; properties used to generate cert key
.text:1022CEE3      loc_1022CEE3:      ; CODE XREF: sub_1022CE70+21fj
                    ; DATA XREF: .text:1022D150+0
.text:1022CEE3      lea     edx, [ebp+phkResult]
.text:1022CEE9      push    edx          ; phkResult
.text:1022CEEA      push    20019h       ; samDesired
.text:1022CEEF      push    0            ; ulOptions
.text:1022CEF1      push    offset aHardwareDescri ; "HARDWARE\\DESCRIPTION\\System"
.text:1022CEF6      push    80000002h    ; hKey
.text:1022CEF8      call    ds:RegOpenKeyExA
.text:1022CF01      test    eax, eax
.text:1022CF03      jnz     loc_1022D135
.text:1022CF09      mov     ecx, [ebp+phkResult]
.text:1022CF0F      mov     edi, ds:RegQueryValueExA
.text:1022CF15      mov     [ebp+cbData], eax
.text:1022CF18      lea     eax, [ebp+cbData]
.text:1022CF21      push    eax          ; lpCbData
.text:1022CF22      push    0            ; lpData
.text:1022CF24      push    0            ; lpType
.text:1022CF26      push    0            ; lpReserved
.text:1022CF28      push    offset aSystembiosvers ; "SystemBiosVersion"
.text:1022CF2D      push    ecx          ; hKey
.text:1022CF2E      call    edi ; RegQueryValueExA
.text:1022CF30      test    eax, eax
.text:1022CF32      jnz     short loc_1022CF85
.text:1022CF34      mov     edx, [ebp+cbData]
.text:1022CF3A      push    edx          ; dwBytes
.text:1022CF3B      push    eax          ; dwFlags
.text:1022CF3C      call    sub_109910E0
.text:1022CF41      push    eax          ; hHeap
.text:1022CF42      call    ds:_imp_HeapAlloc
.text:1022CF48      mov     ecx, [ebp+phkResult]
.text:1022CF4E      mov     esi, eax
.text:1022CF50      lea     eax, [ebp+cbData]
.text:1022CF56      push    eax          ; lpCbData
.text:1022CF57      push    esi          ; lpData
.text:1022CF58      push    0            ; lpType
.text:1022CF5A      push    0            ; lpReserved
.text:1022CF5C      push    offset aSystembiosvers ; "SystemBiosVersion"
```

Key Points



Auto Crawler System

• App Meta info Crawler

01

• App Download Crawler

- initialize
- **Apple ID sign in**
- App purchase
- Sign the APPs

02

• App Crack Server

- iOS device Authorization
- PC Authorization

03

• Best practice

- for Anti-Anti Crawl
- for Apple ID Activation

04

App Download Crawler - Apple ID Sign In(1/6)

- 1. Request Setup Cert from /signSapSetupCert

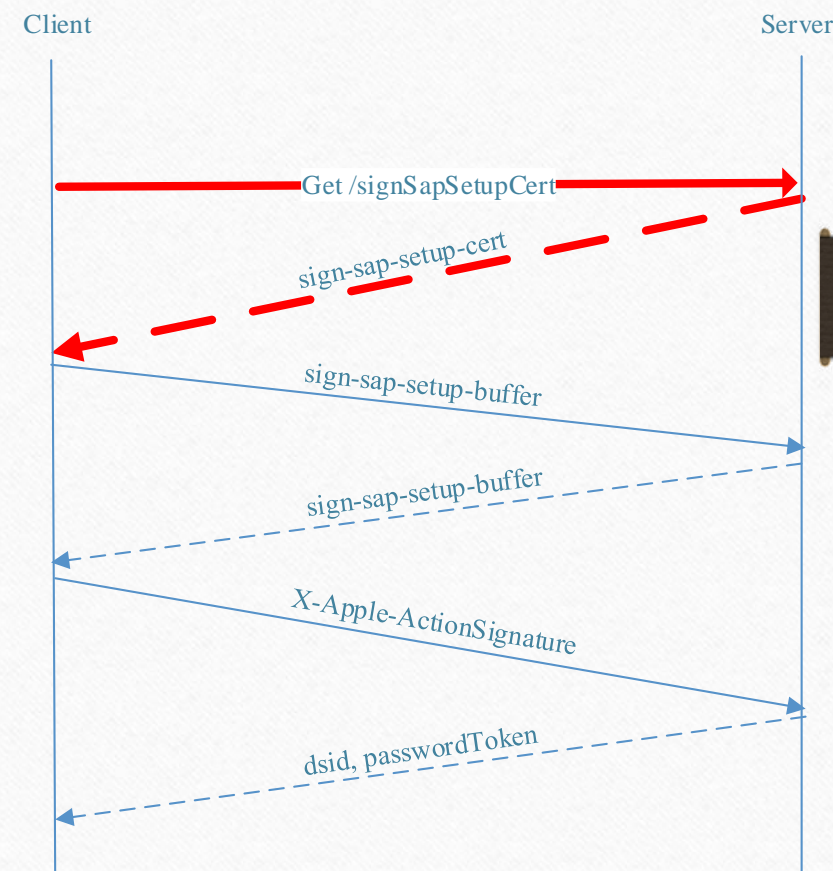
Header Response Content Post Data Request Timing Query String Cookies Raw Stream Hints (3)

text/xml: 3257 bytes **GET /WebObjects/MZInit.woa/wa/signSapSetupCert**

```
- <plist>
- <dict>
  <key>sign-sap-setup-cert</key>

  <data>AQIAAAQWMIEEjCCAvqgAwIBAgIBHDANBgkqhkiG9w0
</dict>
</plist>
```

Header	Response Content	Post Data	Request Timing	Query String	Cookies	Raw Stream	Hints (3)	Comment	Status Code Defi
Request Headers									
(Request-Line)									
Host	init.itunes.apple.com								
Connection	keep-alive								
Accept-Encoding	gzip								
Accept	*/*								
User-Agent	AppStore/2.0 iOS/8.1.3 model/iPhone6,2 build/12B466 (6; dt:90)								
X-Apple-Store-Front	143441-1,17 Region ID								
X-Apple-Tz	28800								



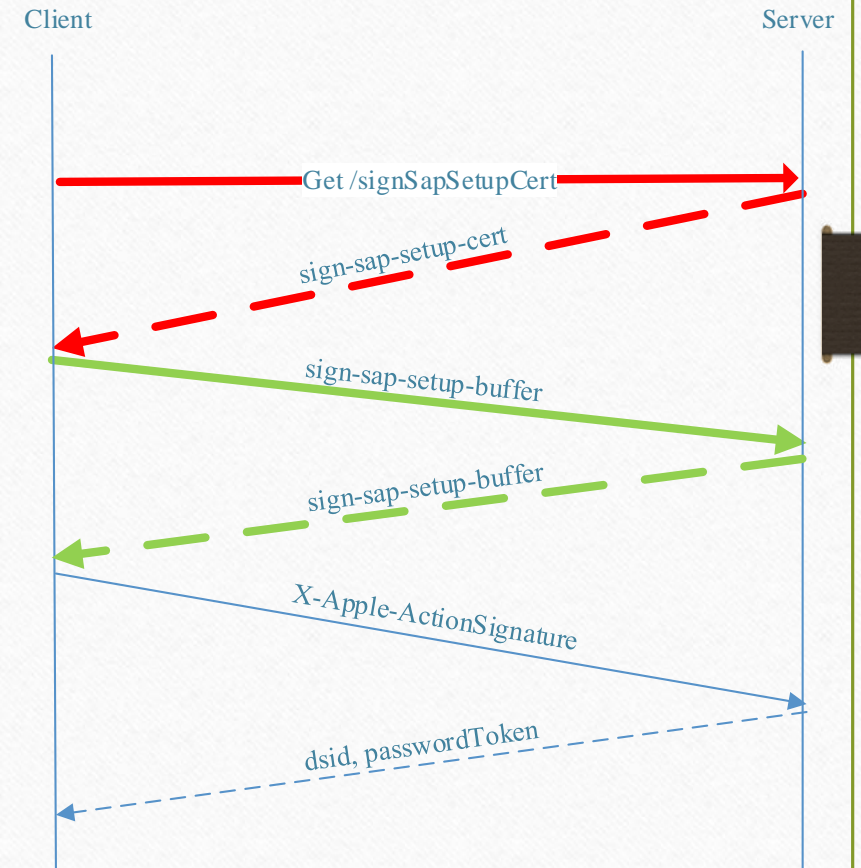
App Download Crawler - Apple ID Sign In(2/6)

- 2. Exchange confirm cert with /signSapSetup
 - Calculated by:
 - Session ID
 - Cert key
 - Setup Cert

Header Response Content Post Data Request Timing Query String Cookies Raw Stream

MimeType: application/x-apple-plist Size: 725 bytes

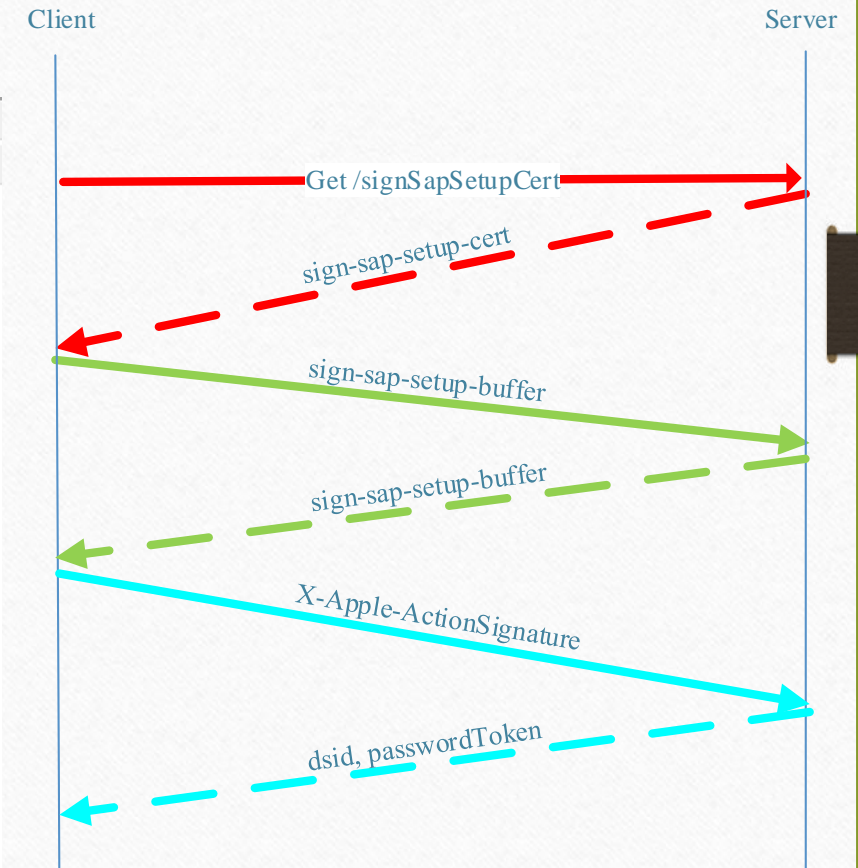
```
/POST WebObjects/MZPlay.woa/wa/signSapSetup  
<?xml version="1.0" encoding="UTF-8" ?>  
<!DOCTYPE plist (View Source for full doctype...)>  
- <plist version="1.0">  
- <dict>  
  <key>sign-sap-setup-buffer</key>  
  <data>AQhKdD/RkztjkITr9Jau6eGokox26e+9eHzCLBH9D9.  
ssLKhtd0ic/Xv3gCQIdqpi5ri0X/Yzy51UVacY+kweTaR8n  
KZWTqowmz5nceiMsOk06/HnN53hVmd7UP+mdXXkC61  
jh7we5RgWvlZuOuBDWzwwox3/ISROd7iVGKK8sU4X29Du  
  </data>  
</dict>  
</plist>
```



App Download Crawler - Apple ID Sign In(3/6)

- 3. Signin Authenticate
 - Post data

```
Header  Response Content  Post Data  Request Timing  Query String  Cookies  Raw Stream  Hints (5)  Comment  Status Code Definition
Mime Type: application/x-apple-plist  Size: 621 bytes
POST /WebObjects/MZFinance.woa/wa/authenticate
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE plist (View Source for full doctype...)>
- <plist version="1.0">
- <dict>
  <key>appleId</key>
  <string>flyicyisheng@gmail.com</string>
  <key>attempt</key>
  <integer>0</integer>
  <key>createSession</key>
  <string>true</string>
  <key>guid</key>
  <string>533EDCA4.8A7893AD.00000000.7B62729A.14DF9387.AB7F7EB4.D588CCEA</string>
  <key>machineName</key>
  <string>ZFBDYQFHMT</string>
  <key>password</key>
  <string>lrjsj2HHRHLID</string>
  <key>rmp</key>
  <string>0</string>
  <key>why</key>
  <string>signIn</string>
</dict>
</plist>
```



App Download Crawler - Apple ID Sign In(4/6)

- GUID is calculated by seven system properties:
 - Network adapter info
 - Volume serial number of 'C:\'
 - System Bios Version
 - CPU info
 - Windows production ID
 - Computer name info
 - Users Hardware profile

App Download Crawler - Apple ID Sign In(5/6)

- 3. Signin Authenticate
 - Post header
 - ActionSignature: calculated by sessionid and post data

[illegible]

App Download Crawler - Apple ID Sign In(6/6)

- The Response of Sign Success

```
Header Response Content Post Data Request Timing Query String Cookies Raw Stream Hints (5) Comment Status Code Definition
text/xml: 1830 bytes
<key>passwordToken</key>
<string>BAIAAAFaAAE45wAAAABbPYzSXV7X+CpaQeOvWYtuMuGMDIn/FB4/UjuR1PxFLuQL
<key>clearToken</key>
<string>30303030303031343932353930303830</string>
<key>m-allowed</key>
<true />
<key>is-cloud-enabled</key>
<string>false</string>
<key>dsPersonId</key>
<string>25176736755</string>
<key>creditDisplay</key>
<string />
<key>creditBalance</key>
<string>1311811</string>
<key>freeSongBalance</key>
<string>1311811</string>
<key>isManagedStudent</key>
<false />
<key>subscriptionStatus</key>
- <dict>
  <key>terms</key>
  - <array>
```

Summary

- Apple ID sign in will bundle your PC's system properties, like GUID, machine name, and so on... However, these information can be fake.

Key Points



Auto Crawler System

• App Meta info Crawler

01

• App Download Crawler

- initialize
- Apple ID sign in
- **App purchase**
- Sign the APPs

02

• App Crack Server

- iOS device Authorization
- PC Authorization

03









• Best practice

- for Anti-Anti Crawl
- for Apple ID Activation

04

App Download Crawler – APPs Purchase Overview

- Contains Following Steps:
 - Step1: Get Purchase URL
 - Step2: Get Essential Properties of Download APPs
 - Step3: Purchase Authenticate
 - Step4: Purchase APPs
 - Step5: Download APPs

4	☆ + 5.672		!	5.297 s	GET	200	130.27 K		https://init.itunes.apple.com/bag.xml?ix=5&dsid=25176736755&ign-bsn=2
5	☆ + 11.500		!	4.344 s	GET	200	463		https://xp.apple.com/register
6	☆ + 21.313		!	9.078 s	POST	200	301		https://upp.itunes.apple.com/WebObjects/MZBookkeeper.woa/wa/getAll
7	☆ + 30.703		!	2.969 s	GET	200	77.28 K		https://itunes.apple.com/us/app/appname/id899247664?mt=8
8	☆ + 33.891		!	0.516 s	POST	200	1.79 K		https://p18-buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/authenticate
9	☆ + 34.672		!	12.969 s	POST	200	12.63 K		https://p18-buy.itunes.apple.com/WebObjects/MZBuy.woa/wa/buyProduct
10	☆ + 48.641		!	602.469 s	GET	200	13.77 M		http://iosapps.itunes.apple.com/apple-assets-us-std-000001/Purple128/v4/37/ed/ce/37
13	☆ + 700.141		!	1.187 s	GET	200	228		https://p18-buy.itunes.apple.com/WebObjects/MZFastFinance.woa/wa/songDownload

APPs Purchase – Get Purchase URL

- GET “/bag.xml?ix=5&dsid=%(dsid)s&ign-bsn=2”
 - Response: all the action URLs

```
<key>songDownloadDone</key><string>https://p52-buy.itunes.apple.com/WebObjects/MZFastFinance.woa/wa/songDownloadDone</string>  
<key>push-notifications</key>  
<dict>  
  <key>register-success</key><string>https://p52-buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/registerSuccess</string>  
  <key>environment</key><string>production</string>  
</dict>  
<key>buyProduct</key><string>https://p52-buy.itunes.apple.com/WebObjects/MZBuy.woa/wa/buyProduct</string>  
<key>iPhoneActivation</key><string>https://albert.apple.com/deviceservices/deviceActivation</string>
```


APPs Purchase – Get Essential Properties

- GET <https://itunes.apple.com/%s/app/appname/id%s?mt=8>

```
    "description": {
      "standard": "The TestFlight app allows testers to install and beta test apps",
    },
    "requiredCapabilities": "armv7 ",
    "offers": [
      {
        "actionText": {
          "short": "Get",
          "medium": "Get",
          "long": "Get App",
          "downloaded": "Installed",
          "downloading": "Installing"
        },
        "type": "get",
        "priceFormatted": "$0.00",
        "price": 0,
        "buyParams": "productType=C&price=0&salableAdamId=899247664&pricingParameter",
        "version": {
          "display": "2.0.2",
          "externalId": 827626291
        },
      },
      {
        "assets": [
          {
            "flavor": "iosSoftware",
            "size": 31648768
          }
        ]
      }
    ]
  }
}
```

APPs Purchase – Purchase Authenticate

- Why: purchase

Header Response Content Post Data Request Timing Query String Cookies Raw Stream Hints (5) Comment Status Code Definition

MimeType:application/x-apple-plist Size:575 bytes

```
POST /WebObjects/MZFinance.woa/wa/authenticate
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE plist (View Source for full doctype...)>
- <plist version="1.0">
- <dict>
  <key>appleId</key>
  <string>flyicyisheng@gmail.com</string>
  <key>attempt</key>
  <integer>1</integer>
  <key>guid</key>
  <string>533EDCA4.8A7893AD.00000000.7B62729A.14DF9387.AB7F7EB4.D588CCEA</string>
  <key>kc</key>
  <integer>1</integer>
  <key>machineName</key>
  <string>ZFB DYQFHMT</string>
  <key>password</key>
  <string>lrysj2HHRHLID</string>
  <key>why</key>
  <string>purchase</string>
</dict>
</plist>
```

Preview

Header Response Content Post Data Request Timing Query String

text/xml: 1830 bytes

```
<string>li</string>
<key>lastName</key>
<string>li</string>
</dict>
</dict>
<key>passwordToken</key>
<string>BAIAAAFaAAE45wAAAABbPY<
<key>clearToken</key>
<string>303030303030313439323539
<key>m-allowed</key>
<true />
<key>is-cloud-enabled</key>
<string>>false</string>
<key>dsPersonId</key>
<string>25176736755</string>
<key>creditDisplay</key>
<string />
<key>creditBalance</key>
<string>1311811</string>
<key>freeSongBalance</key>
<string>1311811</string>
<key>isManagedStudent</key>
```

Preview

APPs Purchase – Purchase APPs(1/3)

- POST Data:

- appExVrsId
 - Got from step2

- Kbsync

- signed by:
 - dsPersonId
 - Keybag

```
pl = {  
  'salableAdamId': str(app_id),  
  'appExtVrsId': str(app_version_id),  
  'guid': self.guid,  
  'machineName': self.machine_name,  
  'needDiv': '1',  
  'mtApp': 'com.apple.iTunes',  
  'mtClientId': '3z4Ci7l8z4Yaz5Dez9lsz1NI2qkA1B',  
  'mtEventTime': str(int(time.time() * 1000)),  
  'mtPageId': '6940a41d-0cde-48ca-b4b0-83a8e94f59ee',  
  'mtPageType': 'Search',  
  'mtPrevPage': 'Genre_29099',  
  'mtRequestId': '3z4Ci7l8z4Yaz5Dez9lsz1NI2qkA1BzJ83V6DURzUKP',  
  'mtTopic': 'xp_its_main',  
  'pg': 'default',  
  'price': '0',  
  'pricingParameters': 'STDQ',  
  'productType': 'C',  
  'kbsync': kbsync_v,  
}
```


APPs Purchase – Purchase APPs(3/3)

- Response of Post

Header Response Content Post Data Request Timing Query String Cookies Raw Stream Hints (5) Comment Status Code Definition

text/xml: 12938 bytes

```
<key>download-queue-item-count</key>
<integer>1</integer>
<key>songList</key>
- <array>
- <dict>
  <key>songId</key>
  <integer>899247664</integer>
  <key>URL</key>
  <string>http://iosapps.itunes.apple.com/apple-assets-us-std-000001/Purple128/v4/37/ed/ce/37edce94-ef9c-1a04-3439-d4b1008e962f/pre-
  thinned8829161187150649132.lc.2496469624430130.7THS7IQPRCR5S.signed.dpkg.ipa?
  accessKey=1530954831_474048049376812077_JxqHZZjUwLUsbOLhjGnkkw6DtuWBhCBPEatVC7xDnXRN25RgoxLg0TqLj7KH3VC0oHwfNf9o79hyq
  2Bs7LfQ1EuSIQg92AL%2B5WcoeTMPzfdeWd3tAvim6L068Ik58g7tH%2FvGXb0XDatsUfPw%2BD8jO%2B9v8Vp%2B%2F%2Bjlu1gJY%2Fjd5CAT
  3D%3D</string>
  <key>downloadKey</key>
  <string>expires=1530954831~access=/apple-assets-us-std-000001/Purple128/v4/37/ed/ce/37edce94-ef9c-1a04-3439-d4b1008e962f/pre-
  thinned8829161187150649132.lc.2496469624430130.7THS7IQPRCR5S.signed.dpkg.ipa*~md5=6fcd6ff2809263e68ecbdd88cc0f99f5</string>
  <key>deltaPackages</key>
+ <array>
  <key>artworkURL</key>
  <string>https://a2.mzstatic.com/us/r30/Purple128/v4/20/91/f1/2091f101-41b1-3758-b299-156bc97c077f/icon1024x1024.jpeg</string>
  <key>artwork-urls</key>
+ <dict>
  <key>is-purchased-redownload</key>
  <true />
```

APPs Purchase – Download APPs(1/2)

- GET SongURL
 - Header: downloadKey

Header	Response Content	Post Data	Request Timing	Query String	Cookies	Raw Stream	Hints (2)	Comment	Status Code Definition
Request Headers					Value				
(Request-Line)					GET /apple-assets-us-std-000001/Purple128/v4/37/ed/ce/37edce94-ef9c-1a04-3439-d4b1008e962f/pre-thinned8829161187150649132.lc.2496469624430130.7THS7IQPRCR5S.signed.dpkg.ipa?accessKey=1530954831_474048049376812077_JxqHZZjUwLUsbOLhjGnkkw6DtuWBhCBPEatVC7xDnXRN25RgoxLg0TqLj7KH3VC0oHwfnf9o79hyq1aWlyBaL6dvEbZOH9EI3AcPM1mgKakagX3CRiLD8EsRa4o40KUFLLEndgKfXltHcdU3u%2Bs7LfQ1EuSIQg92AL%2B5WcoetMPzfdeWd3tAvim6L068Ik58g7th%2FvGXb0XDAtsUfPw%2BD8jO%2B9v8Vp%2B%2F%2Bjlu1gJY%2Fjd5CATevAVkhRv3zcI2T41UgqgWaDJfzBY5HhVij6ugYg%3D%3D HTTP/1.1				
Host					iosapps.itunes.apple.com				
Connection					keep-alive				
Accept-Encoding					gzip, deflate				
Accept					*/*				
User-Agent					python-requests/2.18.4				
Cookie					downloadKey=expires=1530954831~access=/apple-assets-us-std-000001/Purple128/v4/37/ed/ce/37edce94-ef9c-1a04-3439-d4b1008e962f/pre-thinned8829161187150649132.lc.2496469624430130.7THS7IQPRCR5S.signed.dpkg.ipa*~md5=6fcd6ff2809263e68ecbdd88cc0f99f5				

APPs Purchase – Download APPs(2/2)

- Download Status
 - GET songDownloadDone with:
 - songId
 - guid
 - download-id



```
Header Response Content Post Data Request Timing Query String Cookies Raw Stream
text/xml: 228 bytes

<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
- <plist version="1.0">
- <dict>
  <key>pings</key>
  <array />
  <key>jingleDocType</key>
  <string>success</string>
  <key>jingleAction</key>
  <string>null</string>
</dict>
</plist>
```

Summary

- During Apps purchase process, essential properties are needed. However, Kbsync calculation is the key technology.

Key Points



Auto Crawler System

• App Meta info Crawler

01

• App Download Crawler

- initialize
- Apple ID sign in
- App purchase
- **Sign the APPs**

02

• App Crack Server

- iOS device Authorization
- PC Authorization

03

• Best practice

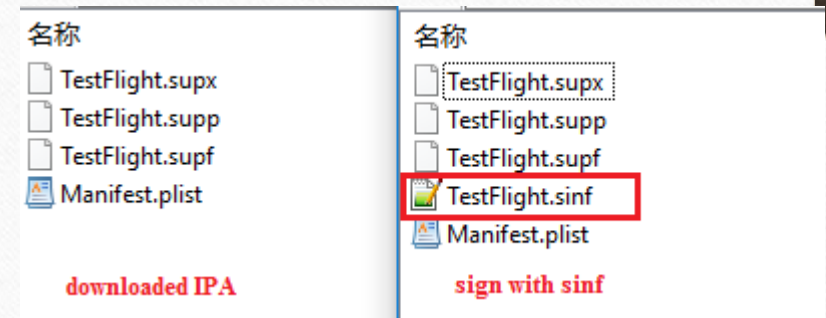
- for Anti-Anti Crawl
- for Apple ID Activation

04

APPs Purchase – Sign APPs

- Sinf: DRM information
- Location: Payload\{*}.app\SC_Info\{*}.sinf

```
<integer>0</integer>  
<key>sinfo</key>  
- <array>  
- <dict>  
  <key>id</key>  
  <integer>0</integer>  
  <key>sinf</key>  
    <data>AAAEFHnpbmYAAAAMZnJtYWdhbWUAAAAUc2NobQAAAABpdHVuAAAAA2Rz  
  </dict>  
</array>
```



Key Points



Auto Crawler System

• App Meta info Crawler

01

• App Download Crawler

- initialize
- Apple ID sign in
- App purchase
- Sign the APPs

02

• App Crack Server

- iOS device Authorization
- PC Authorization

03

• Best practice

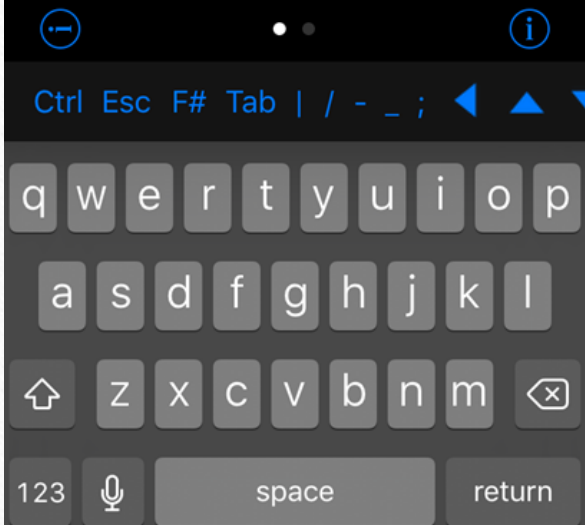
- for Anti-Anti Crawl
- for Apple ID Activation

04

APPS Crack Server – Overview

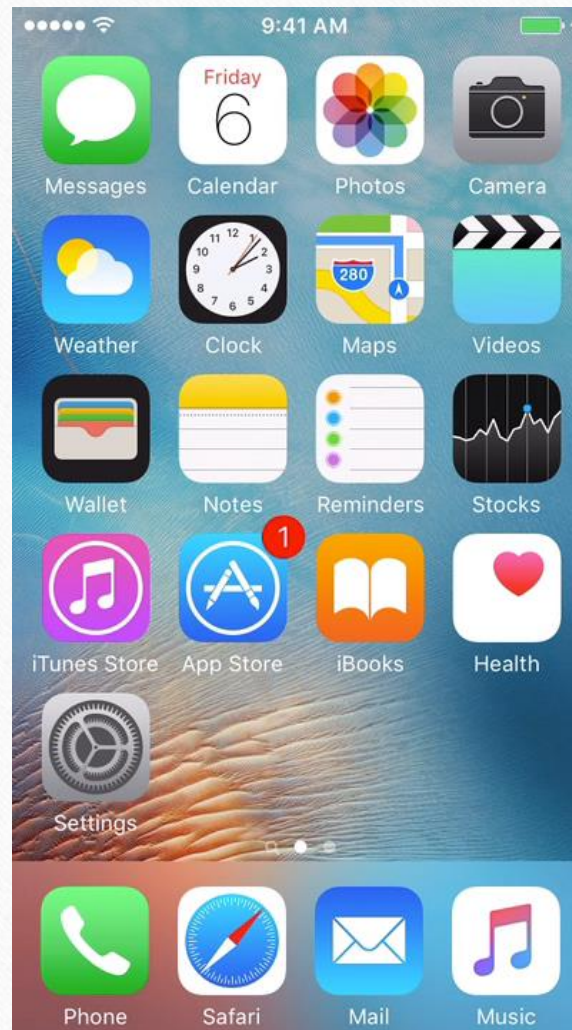
- APPS Crack Server
 - iOS device authorization
 - PC authorization

```
Frankde-iPhone001:/var/mobile root# clutch -i
mars:clutch workingPath=/var/tmp/clutch/D0B1C71C-8CF8
-4700-971E-DC884FF541E3
mars:clutch workingPath=/var/tmp/clutch/70E60F18-552B
-482A-BA4B-573E5FDF9537
mars:clutch workingPath=/var/tmp/clutch/6394C435-6FBB
-4BF4-AE2A-F2DEB59B93F6
Installed apps:
1: A4 Player <com.pd.A4Player>
2: aa cn <com.tmstudio.game.aa>
3: Instagram <com.burbn.instagram>
Frankde-iPhone001:/var/mobile root# clutch -d 2
mars:clutch workingPath=/var/tmp/clutch/DB60B2D6-5A05
-447F-B3C4-F1CEF020494A
mars:clutch workingPath=/var/tmp/clutch/228F4CCF-E3C9
-4CFF-96DA-133C5BF7D84D
mars:clutch workingPath=/var/tmp/clutch/A9B9AE17-1BF9
-459C-AB9A-8C81F4C07B8A
Zipping aa.app
Swapping architectures...
ASLR slide: 0x9c000
Dumping <aa> (armv7)
Patched cryptid (32bit segment)
Writing new checksum
ASLR slide: 0x10008c000
Dumping <aa> (arm64)
Patched cryptid (64bit segment)
```



iDevice authorization

- StoreServices.framework
 - SSAuthenticationContext
 - setAccountName
 - setInitialPassword
 - setPreferredITunesStoreClient

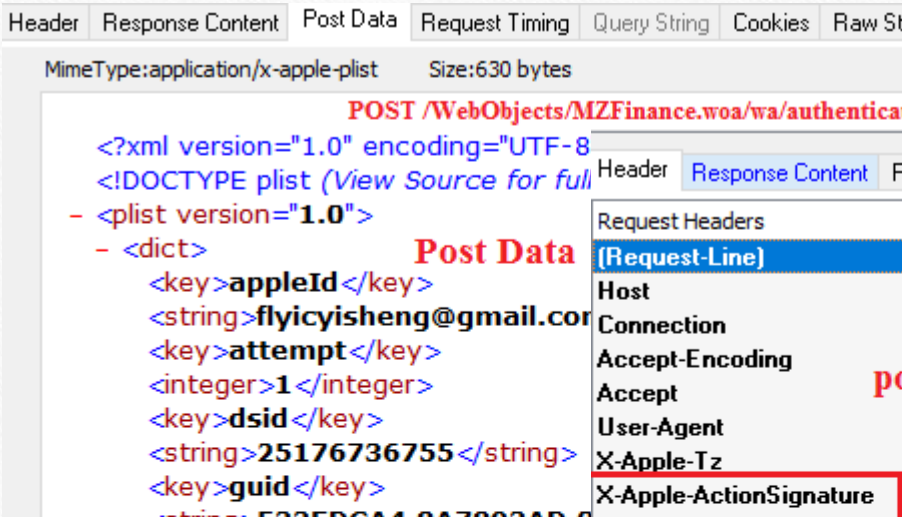


PC authorization

- Two Steps:
 - Machine authorize authenticate
 - Authorize machine

4	+ 2.797		!	0.469 s	POST	200	1.79 K	<>	https://p18-buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/authenticate
5	+ 3.266		!	0.203 s	POST	200	1.47 K	<>	https://p18-buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/authorizeMachine

PC authorization – Step1

- POST /WebObjects/MZFinance.woa/wa/authenticate HTTP/1.1
 - Post data
 - Dsid
 - Why: machineAuthorize
 - Post header
 - ActionSignature
- 
- The screenshot shows the 'Post Data' tab of a web browser's developer tools. The URL is `POST /WebObjects/MZFinance.woa/wa/authenticate`. The MIME type is `application/x-apple-plist` and the size is 630 bytes. The post data is an XML plist structure:
- ```
<?xml version="1.0" encoding="UTF-8"
<!DOCTYPE plist (View Source for full
- <plist version="1.0">
- <dict>
 <key>appleId</key>
 <string>flyicyisheng@gmail.com</string>
 <key>attempt</key>
 <integer>1</integer>
 <key>dsid</key>
 <string>25176736755</string>
 <key>guid</key>
 <string>5235DCA4-8A7802AD-8</string>
```
- The 'Request Headers' tab is also visible on the right, showing the following headers:
- Host
  - Connection
  - Accept-Encoding
  - Accept
  - User-Agent
  - X-Apple-Tz
  - X-Apple-ActionSignature

**POST /WebObjects/MZFinance.woa/wa/authenticate HTTP/1.1**

MimeType: application/x-apple-plist Size: 630 bytes

**Post Data**

```
<?xml version="1.0" encoding="UTF-8">
<!DOCTYPE plist (View Source for full)
- <plist version="1.0">
- <dict>
 <key>appleId</key>
 <string>flyicyisheng@gmail.com</string>
 <key>attempt</key>
 <integer>1</integer>
 <key>dsid</key>
 <string>25176736755</string>
 <key>guid</key>
 <string>533EDCA4.8A7893AD.0</string>
 <key>kc</key>
 <integer>1</integer>
 <key>machineName</key>
 <string>UKAYXWVEFH</string>
 <key>password</key>
 <string>lrysj2HHRHLID</string>
 <key>why</key>
 <string>machineAuthorize</string>
</dict>
</plist>
```

**Request Headers**

| (Request-Line)          | Value                                                                                                      |
|-------------------------|------------------------------------------------------------------------------------------------------------|
| Host                    | p18-buy.it                                                                                                 |
| Connection              | keep-alive                                                                                                 |
| Accept-Encoding         | gzip                                                                                                       |
| Accept                  | */*                                                                                                        |
| User-Agent              | AppStore/                                                                                                  |
| X-Apple-Tz              | 28800                                                                                                      |
| X-Apple-ActionSignature | Avd3Ey53<br>6vN76vN7<br>N76vN76v<br>6vN76vN7<br>N76vN76v<br>6vN76vN7<br>BnUlh1kwL<br>29yVzuAjV<br>mJHmad4S |
| X-Apple-Store-Front     | 143441-1,                                                                                                  |
| Content-Type            | application                                                                                                |
| Cookie                  | wosid=Ge<br>ns-mzf-ins<br>session-st<br>pldftcid=1<br>mz at ss                                             |



# PC authorization – Step2

- POST /WebObjects/MZFinance.woa/wa/authorizeMachine HTTP/1.1
  - guid
  - kbsync

The screenshot displays the developer tools for a POST request to `/WebObjects/MZFinance.woa/wa/authorizeMachine`. The left pane shows the 'Post Data' tab with an Apple Plist XML body. The middle pane shows the 'Request Headers' tab. The right pane shows the 'Response Content' tab with an XML body.

**Post data**

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE plist (View Source for full doctype...)>
- <plist version="1.0">
- <dict>
 <key>guid</key>
 <string>533EDCA4.8A7893AD.00000000.A2</string>
 <key>kbsync</key>
 <data>AAQAA51ksN4tfq6XUpLkpwrCA+i0mJWnlhLTJfFDMZwv0FfgHBni0EMAHBlpJ+Ka</data>
 <key>machineName</key>
 <string>UKAYXWVEFH</string>
 <key>needDiv</key>
 <integer>0</integer>
</dict>
</plist>
```

**Post header**

```
Request Headers
(Request-Line)
Host
Connection
Accept-Encoding
Accept
User-Agent
X-Apple-Tz
X-Token
X-Apple-Store-Front
Content-Type
X-Dsid
Cookie
Content-Length
```

**Post response**

```
text/xml: 1501 bytes
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
- <plist version="1.0">
- <dict>
 <key>pings</key>
 <array />
 <key>jingleDocType</key>
 <string>machineAuthorizationInfoSuccess</string>
 <key>jingleAction</key>
 <string>authorizeMachine</string>
 <key>keybag</key>
 <data>AAgABFFtYxHoJRXZbgoFtQfRfx2OiRgGynbNVYCXPN</data>
</dict>
</plist>
itspod=10; wosid-lite=
mz_at0=25176736755
X-Dsid=25176736755
689
```

# Key Points



## Auto Crawler System

### • App Meta info Crawler

01

### • App Download Crawler

- initialize
- Apple ID sign in
- App purchase
- Sign the APPs

02

### • App Crack Server

- iOS device Authorization
- PC Authorization

03

### • Best practice

- for Anti-Anti Crawl
- for Apple ID Activation

04

## Best practice for Anti-Anti Crawl

Anti-Crawl Methods	Solution
The frequency of accessing Apple Server	1. deploy the download URLs crawler and APPs crawler on different servers
IP	1. Using proxy 2. Using cloud sever, such as AWS
The amount of daily downloads for each PC(GUID)	1. Limit the number of AppleIds bundle with each PC 2. Change GUID in a interval
The total downloads for each Apple ID	1. Set the total downloads threshold value for each Apple ID
The amount of daily downloads for each Apple ID	1. Set the daily downloads threshold value for each Apple ID
Two-Factors authentication mechanism	1. Turn off this features



# Best practice for AppleID Activation

Apple Store Methods	Anti-Methods
Real name or phone number authentication when apply for email address	Apply those email which not need these authentication
Credit card bundle when active Apple ID on idevice	Active account on iTunes, and select 'None' in the bundle step.
IP (IP in that App Store region is need )	Using proxy
Three accounts active limits on each PC	Changing GUID in a interval

# iOS Device Authorization – Case Study(1/2)

- SSAccountStore
- SSAuthenticationContext

```
%hook PreferencesAppController
%new(v)
- (void)signin:(NSString*)appleid password:(NSString*)passwd{
 #pragma clang diagnostic push
 #pragma clang diagnostic ignored "-Wdeprecated-declarations"

 SSAccountStore *currentAccounts = [SSAccountStore defaultStore];
 [currentAccounts signOutAllAccounts];

 SSAuthenticationContext *Context = [SSAuthenticationContext contextForSignIn];
 SSMutableAuthenticationContext *AuthContext = [Context mutableCopy];

 [AuthContext setDemoAccount:true];
 [AuthContext setAccountName:appleid];
 [AuthContext setInitialPassword:passwd];
 [AuthContext setPreferredITunesStoreClient:appleid];

 SSAuthenticateRequest *SignInReq = [[SSAuthenticateRequest alloc] initWithAuthenticationContext:AuthContext];
 if([SignInReq start])
 NSLog(@"Sign in Successfully");
 else
 NSLog(@"Failed");

 #pragma clang diagnostic pop
}
%end
```

# iOS Device Authorization – Case Study(2/2)

- Tweak for the Preferences App
  - Hook PreferencesAppController class

```
%hook PreferencesAppController
- (BOOL)application:(UIApplication *)application didFinishLaunchingWithOptions:(NSDictionary *)launchOptions {
 BOOL flag = %orig;
 #pragma clang diagnostic push
 #pragma clang diagnostic ignored "-Wdeprecated-declarations"
 NSTimer *timer;
 timer = [NSTimer scheduledTimerWithTimeInterval:1.0 target:self selector:@selector(fetchappleid) userInfo:nil repeats:NO];

 #pragma clang diagnostic pop

 return flag;
}
%end
```



Field	Value	Field	Value	Field	Value	Field	Value
1	1.000	2	1.000	3	1.000	4	1.000
5	1.000	6	1.000	7	1.000	8	1.000
9	1.000	10	1.000	11	1.000	12	1.000
13	1.000	14	1.000	15	1.000	16	1.000
17	1.000	18	1.000	19	1.000	20	1.000
21	1.000	22	1.000	23	1.000	24	1.000
25	1.000	26	1.000	27	1.000	28	1.000
29	1.000	30	1.000	31	1.000	32	1.000
33	1.000	34	1.000	35	1.000	36	1.000
37	1.000	38	1.000	39	1.000	40	1.000
41	1.000	42	1.000	43	1.000	44	1.000
45	1.000	46	1.000	47	1.000	48	1.000
49	1.000	50	1.000	51	1.000	52	1.000
53	1.000	54	1.000	55	1.000	56	1.000
57	1.000	58	1.000	59	1.000	60	1.000
61	1.000	62	1.000	63	1.000	64	1.000
65	1.000	66	1.000	67	1.000	68	1.000
69	1.000	70	1.000	71	1.000	72	1.000
73	1.000	74	1.000	75	1.000	76	1.000
77	1.000	78	1.000	79	1.000	80	1.000
81	1.000	82	1.000	83	1.000	84	1.000
85	1.000	86	1.000	87	1.000	88	1.000
89	1.000	90	1.000	91	1.000	92	1.000
93	1.000	94	1.000	95	1.000	96	1.000
97	1.000	98	1.000	99	1.000	100	1.000

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

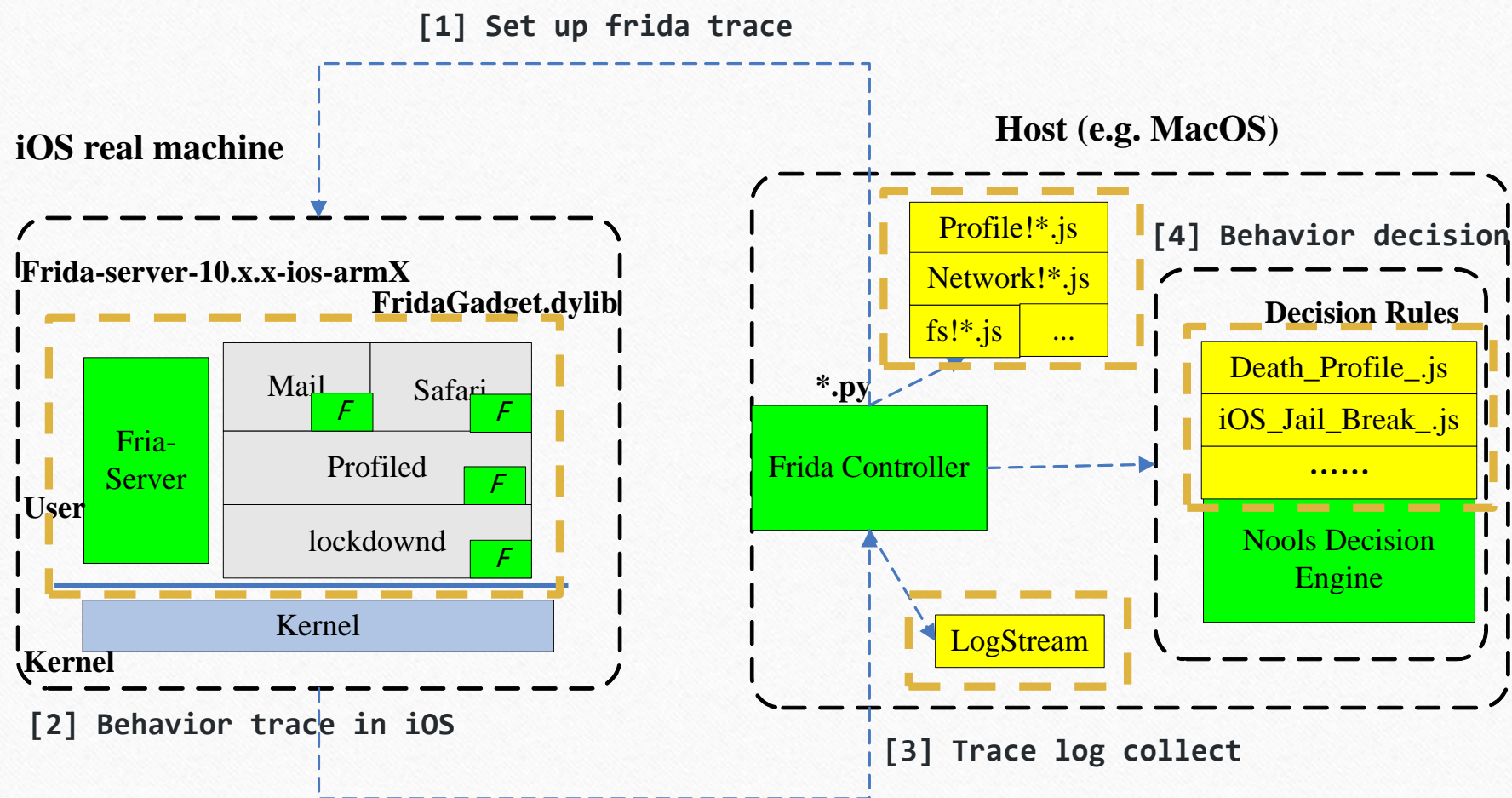
File Edit View Database Tools Window Help

File Edit View Database Tools Window Help

# Sandbox Analysis System

-Real Machine (iOS Device) Sandbox System

# Sandbox based on Frida



USB/Wifi



# Work Flow

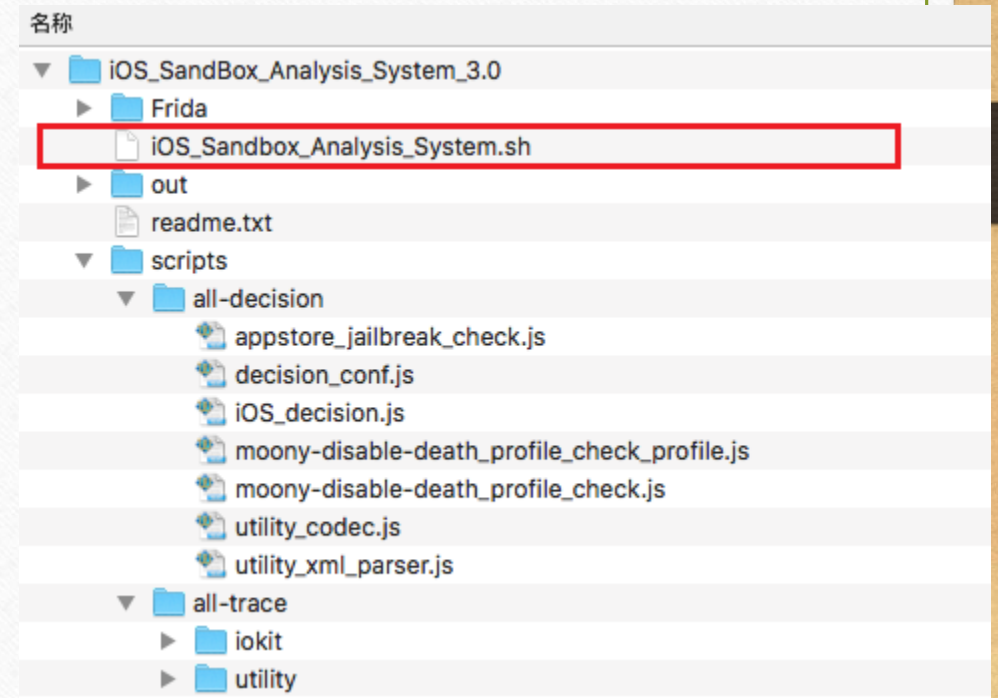
Setup Frida-server in JB/Jailed iOS

Launch customized appmon.py to load script for instrumentation

Save trace log and make decision

# Frida controller

- Controller based on AppMon
  - Python `appmon.py -p $platform -a $targetAppName -s $scriptFolder -o $outDir`
  - Customized `appmon.py`
- Scripts for sandbox rule
  - System trace
    - File, Network, Process, Socket, XPC, Profile, Utility
  - Rule decision
    - E.g. Death profile attack



# Customized appmon.py

- Handle unexpected exception
  - on\_detached, on\_lost, on\_message ...
- Support Multiple processes trace
- Support “wait for” mode (Not graceful but useful☹)

```
try:
 while True:
 self.init_session()
 if self.session and self.device :
 if self.script :
 self.script.on('message', self.on_message)
 self.script.load()
 if self.session:
 break
except Exception as e:
 print colored('[ERROR] ' + str(e), 'red')
 traceback.print_exc()
```





# Sandbox Analysis System

- iOS Application Emulator









# Sandbox Analysis System

- In the Wild Threat Hunt

# Key Points



In the  
Wild  
Threat  
Hunt

• App Meta info Crawler

• PGClient Jail break Tool

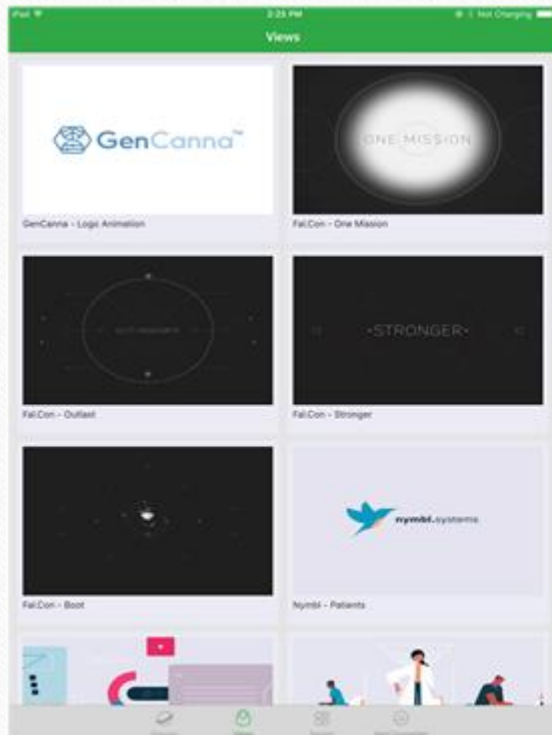
01

• Death Profile Attack

02

# Wild Threat Hunt – PGClient

- Behave as a client of Dribbble





# Wild Threat Hunt – PGClient

- Two identities

```
+ [LoManager load:applicationWillEnterForeground:]
+ [LoManager sharedInstance]
- [LoManager .cxx_destruct]
- [LoManager complete]
- [LoManager setComplete:]
_27_LoManager_sharedInstance__block_invoke
_49_LoManager_load_applicationWillEnterForeground__block_invoke
_49_LoManager_load_applicationWillEnterForeground__block_invoke_2
```

```
objc_release(v58);
objc_release(v56);
v59 = objc_msgSend(&OBJC_CLASS_UIStoryboard, "storyboardWithName:bundle:", CFSTR("Main"), 0LL);
v60 = (void *)objc_retainAutoreleasedReturnValue(v59);
v61 = objc_msgSend(v3, "window");
v62 = (void *)objc_retainAutoreleasedReturnValue(v61);
v63 = objc_msgSend(v60, "instantiateInitialViewController");
v64 = objc_retainAutoreleasedReturnValue(v63);
objc_msgSend(v62, "setRootViewController:", v64);

v3 = objc_msgSend(&OBJC_CLASS__LoManager, "sharedInstance");
v4 = (void *)objc_retainAutoreleasedReturnValue(v3);
objc_msgSend(v4, "setComplete:", *(_QWORD *) (v2 + 32));
objc_release(v4);
v5 = objc_msgSend(&OBJC_CLASS_UIStoryboard, "storyboardWithName:bundle:", CFSTR("JBMain"), 0LL);
v6 = (void *)objc_retainAutoreleasedReturnValue(v5);
v7 = objc_msgSend(&OBJC_CLASS_UIApplication, "sharedApplication");
v8 = (void *)objc_retainAutoreleasedReturnValue(v7);
v9 = v8;
v10 = objc_msgSend(v8, "delegate");
```

```
- [OSCTabBarController .cxx_destruct]
- [OSCTabBarController addNavigationItemForViewController:]
- [OSCTabBarController didReceiveMemoryWarning]
- [OSCTabBarController onClickMenuButton]
- [OSCTabBarController viewDidLoad]
```

















```
- [vFEWwE41k0wRdF4dQ64wyWB installPPHelper]
- [vFEWwE41k0wRdF4dQ64wyWB ioCf6tW924HoDh:]
- [vFEWwE41k0wRdF4dQ64wyWB isFirstJb]
- [vFEWwE41k0wRdF4dQ64wyWB jbStatus]
- [vFEWwE41k0wRdF4dQ64wyWB kBZ1cYQCmoUc2]
- [vFEWwE41k0wRdF4dQ64wyWB mLwXhnEjtZ6caSlaSbntBeRvjvQtex.]
- [vFEWwE41k0wRdF4dQ64wyWB nZqDvagstz5U1EnUbJrOsYgWpPpDa]
- [vFEWwE41k0wRdF4dQ64wyWB pl55sc1knsGVFmFd]
- [vFEWwE41k0wRdF4dQ64wyWB ppDownError]
- [vFEWwE41k0wRdF4dQ64wyWB ppDownFinish]
- [vFEWwE41k0wRdF4dQ64wyWB ppPathUrl]
- [vFEWwE41k0wRdF4dQ64wyWB qjdZoKyM7iV74jWgHs40oCCII2QJYN]
- [vFEWwE41k0wRdF4dQ64wyWB resourceConfigDic]
- [vFEWwE41k0wRdF4dQ64wyWB ryxOfboD716UqIPqF34bghoFvg8j8hz]
- [vFEWwE41k0wRdF4dQ64wyWB setCyDownError:]
- [vFEWwE41k0wRdF4dQ64wyWB setCyDownFinish:]
- [vFEWwE41k0wRdF4dQ64wyWB setCyPathUrl:]
- [vFEWwE41k0wRdF4dQ64wyWB setDelegate:]
- [vFEWwE41k0wRdF4dQ64wyWB setInstallPPHelper:]
- [vFEWwE41k0wRdF4dQ64wyWB setIsFirstJb:]
```

- Actually, it is a jailbreak tool

```
objc_msgSend(v35, v41, v44, v45);
if ((unsigned int)lpe_action(
 *(_QWORD *)&v2->NSObject_opaque[v37],
 *(_DWORD *)&v2->NSObject_opaque[v38],
 *(const void **)&v2->NSObject_opaque[OBJC_IVAR__vFEWwE41k0wRdF4dQ64wyWB__second_data],
 *(_DWORD *)&v2->NSObject_opaque[OBJC_IVAR__vFEWwE41k0wRdF4dQ64wyWB__second_size]))
 v46 = "p155sc1knsGVFmFd";
else
 v46 = "kBZ1cYCQmoUc2";
```

#### Functions list

Function name

	bj
	l
	bk
	bh
	ac
	bq
	bc
	w
	bi
	ce
	ab
	ap
	av
	bf
	n
	y

```
qword_100328B30 = az(
 de,
 df,
 (unsigned int)cx);
qword_100328B40 = ac(
 de,
 df,
 (unsigned int)cx);
qword_100328B38 = w(
 de,
 df,
 (unsigned int)cx);
qword_100328B48 = 0LL;
v404 = bg(*v1368); // start jailbreaking
*v1343 = v404;
v405 = bl();
v470 = bt(v405);
 bu();
 ae(*v1364, (unsigned int)ek);
v406 = IOServiceClose((unsigned int)g_connection);
*v1341 = *v1343; // jailbreak results
v1338 = 862725477;
v469 = v406;
```

- iOS 9.2-9.3.3, known as "NüwaStone" (CVE-2016-4654)

```
io_connect_t conn = IOServiceOpen("AppleCLCD");

uint32_t count = 0xdeaddead;

uint64_t swapIORequestID = 0;

uint32_t swapIDSize = 1;

IOConnectCallScalarMethod(conn, 4, 0, 0, &swapIORequestID, &swapIDSize);

struct IOMFBSwap_obj ss = {0};

ss.swapID = swapIORequestID;

ss.enabled = -1;

ss.completed = 0;

ss.count = count;

IOConnectCallScalarMethod(g_connection, 5, &ss, sizeof(ss), 0, 0);
```





# Key Points



In the  
Wild  
Threat  
Hunt

• App Meta info Crawler

• PGClient Jail break

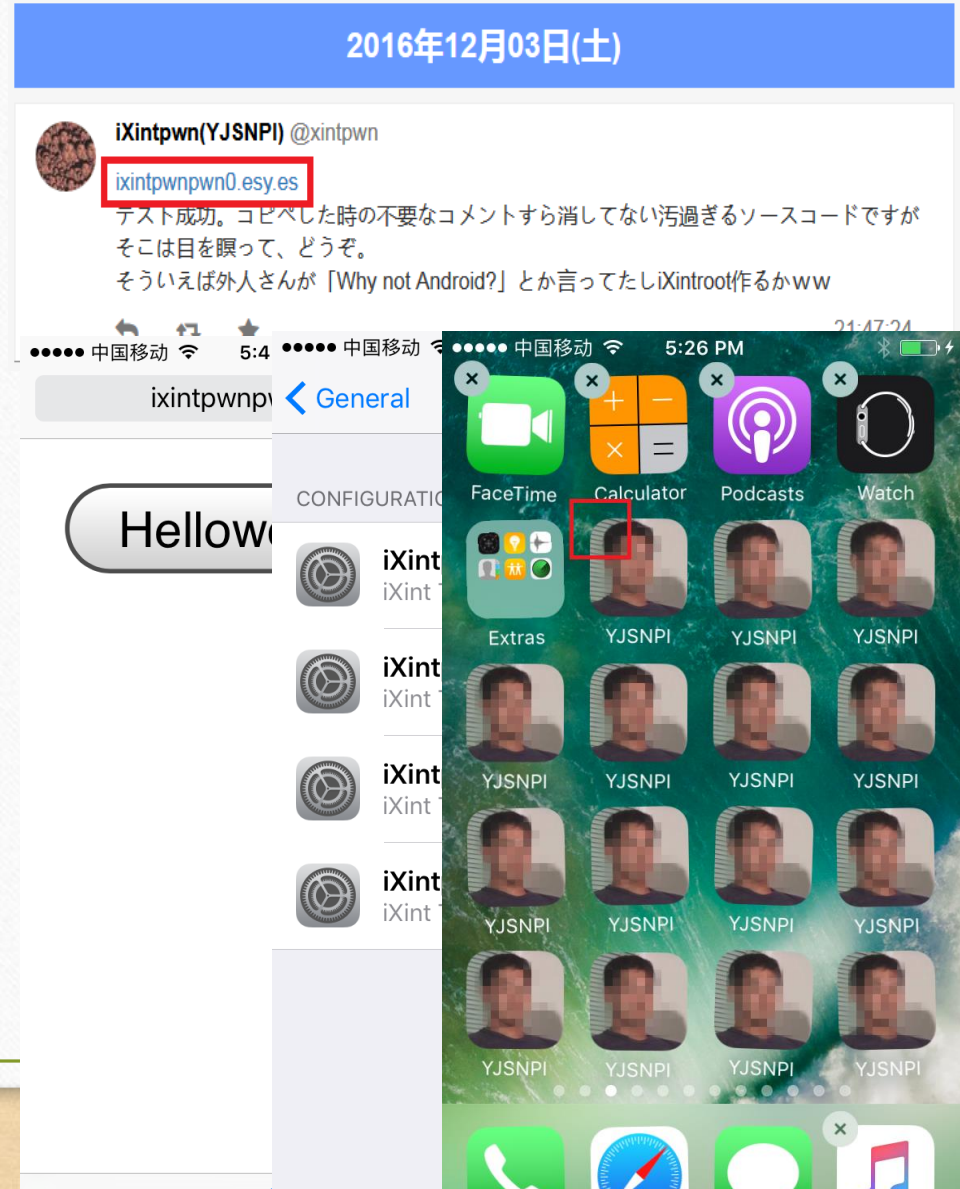
01

• Death Profile Attack

02

# Tricks to scare users

- Attack vector by twitter
- Lure to install profile
  - Web URL via Safari
  - Attachment in Mail
- SpringBoard Icon scare
  - Hundreds of rubbish Icon
  - WebClip unmovable
  - Demo or prototype



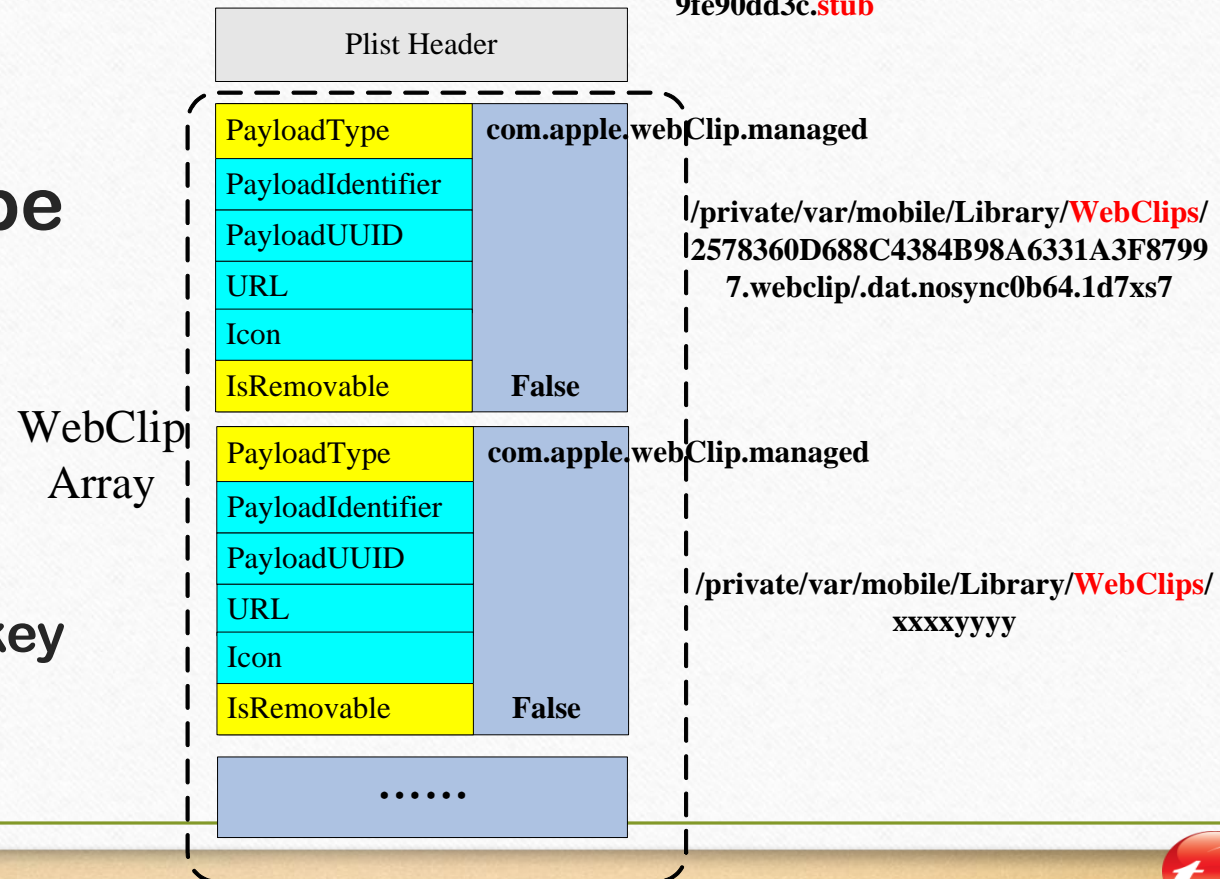


# Mobile profile

- Mobile profile
  - \*.mobileconfig
  - PayloadType
- WebClips Array
  - Un-removable key
  - Unlimit

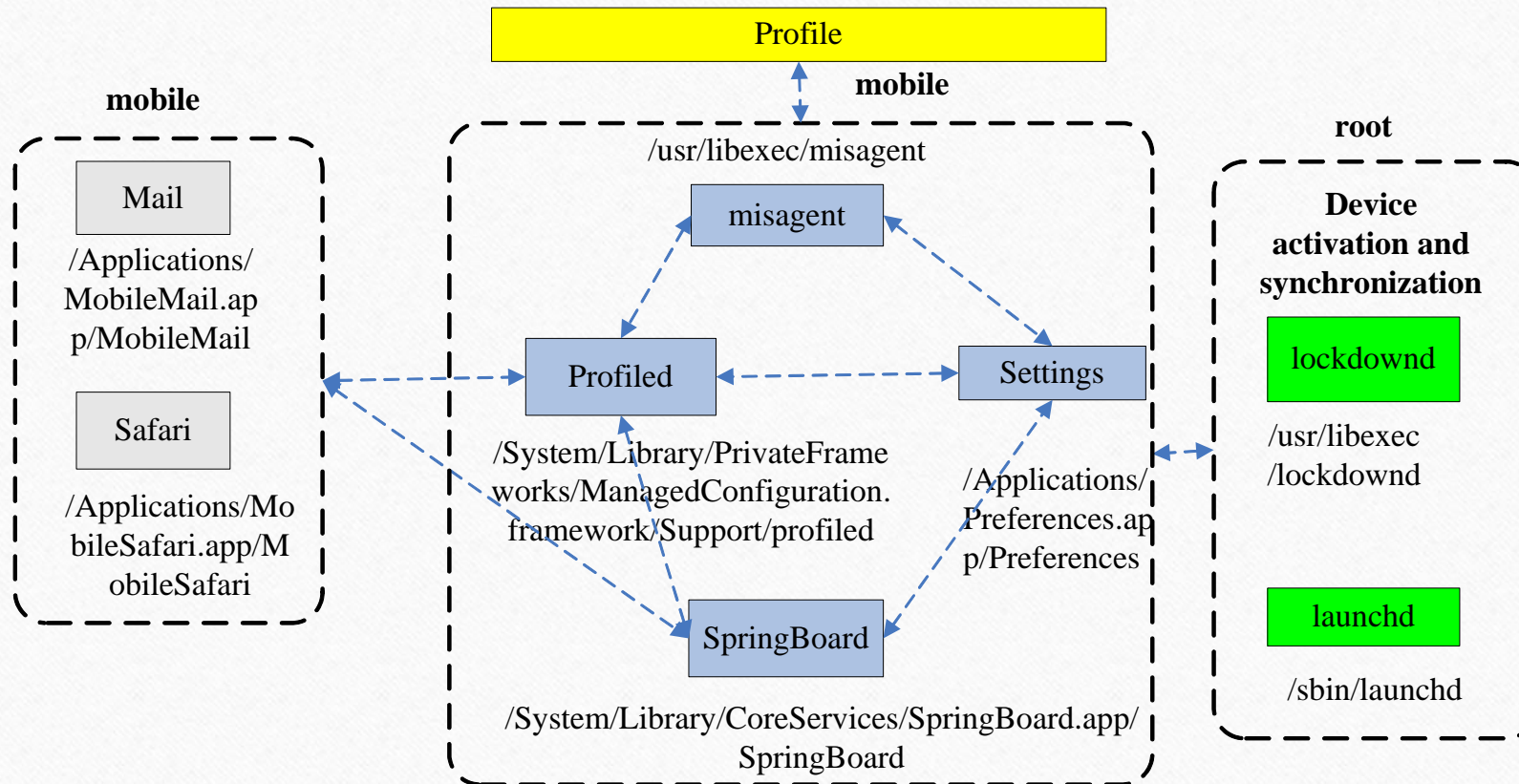
\*.mobileconfig  
XML/Plist format like

/private/var/mobile/Library/ConfigurationProfiles/**profile-**  
4ecba0b5def636872b1da380625  
035b4adfb4c5f4f38788cf177457  
9fe90dd3c.**stub**



# Profile install relationship

/private/var/mobile/Library/ConfigurationProfiles/profile-4ecba0b5def636872b1da380625035b4adfb4c5f4f38788cf1774579fe90dd3c.stub



Profiled ↔ misagent

xpc\_connection\_get\_name\_by\_address: com.apple.misagent

[2916:289299 (profiled)]: libxpc.dylib!xpc\_connection\_send\_message\_with\_reply\_sync : connection=0x1575c100

connectionName=com.apple.misagent connectionPid=3115 connectionProcName=misagent

[2916:205566 (profiled)]: libsystem\_kernel.dylib!\_\_read\_nocancel call stack:

0x26032dcb Foundation!\_NSReadFromFileDescriptorWithProgress,

0x26032c11 Foundation!\_NSReadBytesFromFileWithExtendedAttributes,



# Basic flow in detail

- Safari->SpringBoard/Settings->Profiled  
->Misagent

```
35757 ms -[MCInstaller installProfileData:0x4dd000 options:0x0 interactionClient:0x17e1f170 outError:0x1f102ec0]
35774 ms -[MCInstaller installProfileHandler:0x17d41500 options:0x17e93f50 interactionClient:0x17e1f170 outError:0x1f102e54]
[1749:46650 (profiled)]:libxpc.dylib!xpc_connection_create: name=com.apple.misagent
call stack:
0x38c4429d libxpc.dylib!xpc_connection_create_mach_service,
0x3831c701 libmis.dylib!0x2701,
0x3831c8f1 libmis.dylib!MISEnumerateInstalledProvisioningProfiles,
0x5cb2f profiled!0x55b2f,
0x4631d profiled!0x3f31d,
0xbf85 profiled!0x4f85,
0x38a6cd2b libdispatch.dylib!_dispatch_call_block_and_release,
0x38a7992b libdispatch.dylib!_dispatch_queue_drain$VARIANT$mp,
0x38a78f69 libdispatch.dylib!_dispatch_queue_invoke$VARIANT$mp,
0x38a7baf1 libdispatch.dylib!_dispatch_root_queue_drain,
0x38a7b4d5 libdispatch.dylib!_dispatch_worker_thread3,
0x38c26b45 libsystem_pthread.dylib!_pthread_wqthread
```



# Key trace log

call stack:

```
0x24a52dcb Foundation!_NSReadFromFileDescriptorWithProgress,
0x24a52c11 Foundation!_NSReadBytesFromFileWithExtendedAttributes,
0x24a528ad Foundation!-[NSData(NSData) initWithContentsOfFile:],
0x24a57f33 Foundation!+[NSData(NSData) dataWithContentsOfFile:],
0x2db263d3 ManagedConfiguration!+[MCManifest installedProfileDataWithIdentifier:],
0x2db2629d ManagedConfiguration!+[MCManifest installedProfileWithIdentifier:],
0xa8873 profiled!0x59873,
0xa9ca1 profiled!0x5aca1,
0x9a3f3 profiled!0x4b3f3,
0x9bf11 profiled!0x4cf11,
0x53f2d profiled!0x4f2d,
0x35ca4d2b libdispatch.dylib!_dispatch_call_block_and_release,
0x35cb192b libdispatch.dylib!_dispatch_queue_drain$VARIANT$mp,
0x35cb0f69 libdispatch.dylib!_dispatch_queue_invoke$VARIANT$mp,
0x35cb3af1 libdispatch.dylib!_dispatch_root_queue_drain,
0x35cb34d5 libdispatch.dylib!_dispatch_worker_thread3
{"time":"2017-08-30T05:05:37.526Z","txnType":"syscall","lib":"libsystem_kernel.dylib","method":"read","artifact":[{"name":"filePath","value":"/private/var/mobile/Library/ConfigurationProfiles/profile-4ecba0b5def636872b1da380625035b4adfb4c5f4f38788cf1774579fe90dd3c.stub"},"argSeq":0}]
```

# Key decision rule

```
exports.deathProfileCheckProfileByObjJson = function(plistObj)
{ //traverse(plistObj).forEach(function (x)
 if (&& payload.hasOwnProperty("PayloadType")
 && -1 < payload.PayloadType.search('com.apple.webClip.managed'))
 { payloadTemp.PayloadType = payload.PayloadType;
 if (payload.hasOwnProperty("IsRemovable"))
 {
 if (payload.IsRemovable == false)
 { payloadTemp.IsRemovable = payload.IsRemovable;
 payloadTemp.score = decision_conf.MALICIOUS_VALUE;
 }
 }
 }
 else if (evidenceInBrief.hasOwnProperty("PayloadRemovalDisallowed"))
 {
 if (evidenceInBrief.PayloadRemovalDisallowed == 1)
 { payloadTemp.score = decision_conf.MALICIOUS_VALUE;
 }
 }
}
```



Q&A