Now iOS has been compromised to Suspected Ransomware

Ju Zhu, @ju__zhu
Moony Li, @Flyic
What We Will Cover

• Who We Are
• Story of iOS Profile Ransomware
• Technical Analysis
• Detection Solution
• Demo
Who We Are
Ju Zhu
- @ju__zhu
- 5+ years mobile security
- Mobile Advanced Threat Research
- Hunt Mobile 0Day/nDay
- Mobile Vulnerability
Moony Li

- @Flyic
- 8 years security
- Sandcastle
- Deep Discovery
- Exploit Detection
- Mac/Windows Kernel
- iOS/Android Vulnerability
Story of iOS Profile Ransomware
Attack Vector by Twitter

• Version 1.0 Appears (2016/11)

2016年11月25日(金)

iXintpwn(YJSNPl) @xintpwn
@4_1_I7_3_1V
そんな風に表示されるんかwwwPCだとただの四角にしかならない
@4_1_I7_3_1V への返信

iXintpwn(YJSNPl) @xintpwn
@4_1_I7_3_1V
非常にスッキリやり方で見つけた pic.twitter.com/36V1mj0AKz
@4_1_I7_3_1V への返信

iXintpwn(YJSNPl) @xintpwn
@xintpwn
ixintpwn.zohosites.com
@xintpwn への返信

Jailbreak for iOS9.3.2-
10.1.1(64/32bit)
iXint Team
provide
Jailbreak for
everyone

Download iXintpwn
The Source Code Released (Next Day)

iOS野獣先輩増殖ウィルスを解析して遊べるようにしたもの https://83anija.github.io/iosconshock...

iXintpwn Tester

このサイトは83兄者がiXintpwnのソースを適当に見て勝手にjavascriptで動的生成できるようにしたものです。

まだガバガバソースなので堂々と公開はないです。みたけどソースたどってください。
一応オブジェクト化してしまって改変も作れるようになりました。

なおここで生成されるプロファイアルは本家同様ホーム画面に大量に野獣先輩が生成され、もしかしたら消せないという超めんどくさい仕様です。
自己責任で使ってください。
俺は説明したので利用者はそれを理解の上で使用したものとします。

ダウンロード

アイコン個数 15

ver1.1
Attack Vector by Twitter

• Version 2.0 Released (2016/12)
Tricks to Scare Victims

• SpringBoard Icon Scare
  • Hundreds of Rubbish Icon
  • WebClip Un-Removable
  • Demo or Prototype
Variation in Third-Party Store

- Third-Party Apple Store
  - 51苹果助手

- Signed Profile
  - Reduce Alert to User

- App Promotion
  - WebClip Un-Removable
Others

• iTunes’s Risk
  • Auto Sync
• Provision Profile
  • Bypass Establish Trust
Technical Analysis
Technical Analysis

- Mobile Config Profile
- Profile Install
Mobile Profile

- Mobile Profile
  - `*.mobileconfig`
  - PayloadType
- WebClip Array
  - Un-Removable Key
  - Un-Limit

### XML/Plist format like:

```
Plist Header
PayloadType: com.apple.webClip.managed
PayloadIdentifier
PayloadUUID
URL
Icon
IsRemovable: False

PayloadType: com.apple.webClip.managed
PayloadIdentifier
PayloadUUID
URL
Icon
IsRemovable: False
```

### PayloadType

<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>PayloadContent</td>
<td>Array</td>
<td>Array of payload dictionaries.</td>
</tr>
<tr>
<td>PayloadDescription</td>
<td>String</td>
<td>A description of the profile, shown on the Detail screen for the profile.</td>
</tr>
<tr>
<td>PayloadDisplayName</td>
<td>String</td>
<td>A human-readable name for the profile.</td>
</tr>
<tr>
<td>PayloadIdentifier</td>
<td>String</td>
<td>This string is used to determine whether a new profile should replace an existing one or should be added.</td>
</tr>
<tr>
<td>PayloadOrganization</td>
<td>String</td>
<td>A human-readable string containing the name of the organization that provided the profile.</td>
</tr>
<tr>
<td>PayloadUUID</td>
<td>String</td>
<td>A globally unique identifier for the profile.</td>
</tr>
<tr>
<td>PayloadRemovalDisallow</td>
<td>Boolean</td>
<td>If present and set to true, the user cannot delete the profile.</td>
</tr>
<tr>
<td>PayloadType</td>
<td>String</td>
<td>The only supported value is Configuration.</td>
</tr>
<tr>
<td>PayloadVersion</td>
<td>Integer</td>
<td>The version number of the profile format.</td>
</tr>
</tbody>
</table>

### WebClip Array

```
PayloadType
PayloadVersion
PayloadIdentifier
PayloadUUID
URL
Icon
IsRemovable
```

### Key

<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>PayloadType</td>
<td>String</td>
<td>The payload type.</td>
</tr>
<tr>
<td>PayloadVersion</td>
<td>Integer</td>
<td>The version number of the individual payload.</td>
</tr>
<tr>
<td>PayloadIdentifier</td>
<td>String</td>
<td>A reverse-DNS-style identifier for the specific payload.</td>
</tr>
<tr>
<td>PayloadUUID</td>
<td>String</td>
<td>A globally unique identifier for the payload.</td>
</tr>
<tr>
<td>PayloadDisplayName</td>
<td>String</td>
<td>A human-readable name for the profile payload.</td>
</tr>
<tr>
<td>PayloadDescription</td>
<td>String</td>
<td>A human-readable description of this payload.</td>
</tr>
<tr>
<td>PayloadOrganization</td>
<td>String</td>
<td>A human-readable string containing the name of the organization that provided the profile.</td>
</tr>
<tr>
<td>URL</td>
<td>String</td>
<td>The URL that the Web Clip should open when clicked.</td>
</tr>
<tr>
<td>Label</td>
<td>String</td>
<td>The name of the Web Clip as displayed on the Home screen.</td>
</tr>
<tr>
<td>Icon</td>
<td>Data</td>
<td>A PNG icon to be shown on the Home screen.</td>
</tr>
<tr>
<td>IsRemovable</td>
<td>Boolean</td>
<td>If false, the web clip is unremovable.</td>
</tr>
</tbody>
</table>
Remote Entry for Profile Installation

• How did the author do it?
  • Template
  • Multiple Installations

```javascript
var length = 8
var randomID = Math.random().toString(36).slice(-length);
value2 = insertStr(res, 377, randomID);

function insertStr(str, index, insert) {
  return str.slice(0, index) + insert + str.slice(index, str.length);
}

function submitReq1() {
  XMLHttpRequestオブジェクト取得
  httpObj1 = createHttpObject();
  if (httpObj1) {
    // GETメソッドでrequest1を実行
    httpObj1.open("GET", "ixint1.
    httpObj1.onreadystatechange = textSave('myfile', value2);
    if (httpObj1.readyState == 4) {
      // 正常に受信完了できたとき読み
      var res = httpObj1.responseText;
    }
  } else {
    document.write(value2)
  }

  function textSave(name, text) {
    var blob = new Blob([text], {type: 'application/x-apple-aspen-config'});
    var link = document.createElement('a')
    link.href = URL.createObjectURL(blob);
    link.download = name + '.mobileconfig'
    link.click()
  }
```
Basic Install Flow

1. Trigger Profiled for Installation
2. Interact with “Settings”
3. Profiled Handling
4. XPC Escalation to High Privilege Process
Trigger Profiled for Installation

- Safari -> Profiled

```
Frida hook libxpc.dylib/libxpc_connection_create
libxpc.dylib/libxpc_connection_create: name=com.apple.managedconfiguration.profiled

call stack:
0x3429029d libxpc.dylib/libxpc_connection_create_mach_service,
0x22e45dfd Foundation!-[NSXPCConnection initWithMachServiceName:options:],
0x2bf31323 ManagedConfiguration!-[MCProfileConnection_queueCreateAndResumeXPCConnection],
0x2bf310d1 ManagedConfiguration!_36-[MCProfileConnection xpcConnection]_block_invoke,
0x340b8d17 libdispatch.dylib/libdispatch_client_callout,
0x340c4525 libdispatch.dylib/libdispatch_barrier_sync_f_invoke,
0x2bf3106b ManagedConfiguration!-[MCProfileConnection xpcConnection],
0x2bf6c2f9 ManagedConfiguration!-[MCProfileConnection(Profiles)_queueDataForAcceptance:originalFileName:originatingBundleId:transitionToUI:outError:],
0x2bf6c6ad ManagedConfiguration!-[MCProfileConnection(Profiles) queueFileDataForAcceptance:originalFileName:outError:],
0xa1e1d MobileSafari!0xe4ce1d,
0x25cd6ab9 SafariServices!-[SFDownloadController_downloadDidFinish],
0x162a39 MobileSafari!0x10da39,
0x26e0f2e9 WebKit!WebKit::DownloadClient::didFinish(WebKit::WebProcessPool*, WebKit::DownloadProxy*),
0x26e1114f WebKit!WebKit::DownloadProxy::didFinish(),
0x26e2acc9 WebKit::IPC::MessageReceiverMap::dispatchMessage(IPC::Connection&, IPC::MessageDecoder&),
0x26e4a743 WebKit!WebKit::NetworkProcessProxy::didReceiveMessage(IPC::Connection&, IPC::MessageDecoder&)```
Interact with “Settings”

- Profiled -> Settings
  - “com.apple.Preferences”
  - Interact with User
Profiled Handling

- Profile Handle
  - “profile-xxxxxxxxxxxxxxxxxxxxx.stub”
- WebClip Number Un-Limit
- a Buggy Module
Escalation to High Privilege Process

- Profiled -> Misagent

[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
Profile Install Relationship

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

Profile Install Relationship Diagram

Profile

mobile

Mail
/Applications/MobileMail.app/MobileMail

Safari
/Applications/MobileSafari.app/MobileSafari

Profiled
/System/Library/PrivateFrameworks/ManagedConfiguration.framework/Support/profiled

misagent
/usr/libexec/misagent

Profile
domobile

Settings
/Applications/Preferences.app/Preferences

SpringBoard
/System/Library/CoreServices/SpringBoard.app/SpringBoard

Device activation and synchronization
lockdownd
/usr/libexec
/sbin/launchd

launchd
/sbin/launchd

Mail
launchd

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,
New Remote Attack Interface

• Reason
  • Bypass Apple Store Security Audit
  • Safari->Profiled->Misagent->Lockdown(Root)

• Vulnerabilities Hunt
  • Profiled and Other System Process Heap Overflow
  • Enterprise Certificate App Trust Vulnerability
SpringBoard Crash

- WatchDog’s Timeout
Issue Analysis

- High CPU
- Null Pointer
- Dead Loop
Solution to Detection

- Local VPN
- Sandbox Based on Frida
VPN Setting

VPN CONFIGURATIONS

Status: Connected

"Content Shield Protection" will connect on demand.

- Content Shield Protection
  Mobile Security

Add VPN Configuration...
Solution for Detection

• Local VPN
  • Network Extension Framework Ever Since iOS 8+

• Dynamic Sandbox
  • Jail-Break iOS Devices
  • FridaGadget.dylib Injection
  • JS Behavior Rules
  • Nools Decision Engine
Local VPN Solution

Technically we can obtain raw TCP/UDP traffic

HTTP(s) Traffic

Raw TCP/UDP Traffic

Start a Local VPN Tunnel

iTMMS

Local HTTP Proxy Server

TCP/UDP Handler (YITM)

System Default

WTP Module

Network Extension
Local VPN

*.mobileconfig Pattern

Traffic Filter for File Element

VPN Extension
Sandbox Based on Frida

[1] Set up frida trace

iOS real machine

Frida-server-10.x.x-ios-armX
FridaGadget.dylib

User

Fria- Server

Kernel

Mail  F  Safari  F

Profiled  F

lockdownd  F

Kernel

[2] Behavior trace in iOS

[3] Trace log collect

[4] Behavior decision

Host (e.g. MacOS)

Frida Controller

Profile!*.*.js
Network!*.*.js
fs!*.*.js
...

LogStream

Decision Rules

Death_Profile_.js
iOS_Jail_Break_.js
...

Nools Decision Engine

USB/Wifi

[2] Behavior trace in iOS
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}}}
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;
        }
    }
}
What We Will Cover

• Death Profile Attack Demo
• Sandbox Detection Demo
Thanks very much