ENTERPRISE APPS:
BYPASSING THE IOS GATEKEEPER

Ohad Bobrov
Avi Bashan
AGENDA

- iOS Ecosystem overview
- Enterprise Apps in the iOS Ecosystem
- Bypassing the Gatekeeper
- Conclusions
- Q&A
ABOUT US

OHAD BOBROV
• Over a decade of experience researching and working in the mobile security space
• Former Founder & CTO @Lacoon Mobile Security
• Mobile Threat Prevention Area Manager @Check Point

AVI BASHAN
• Security researcher for over a decade in the PC and mobile areas
• Former CISO & Security Researcher @Lacoon
• Mobile Dynamic Analysis Team Leader @Check Point
THE iOS ECOSYSTEM

IOS IS A MODERN OPERATING SYSTEM

- Sandboxing capabilities
- Resources access requires permission
- Signed code verification

MANAGED APP PUBLISHING PROCESS

- Central App Store
- Developer registration is required to publish apps
- Anonymous development is not allowed
APPLE’S APP REVIEW PROCESS

EVERY APP PUBLISHED TO THE APP STORE IS REVIEWED

- Automatic process
- Manual Process

APP STORE REVIEW GUIDELINES INCLUDES

- App content
- App behavior
- Bugs
- API abuse
- And more
APPLE DEVELOPER ENTERPRISE PROGRAM

MOTIVATION

- Exposure of proprietary In-House Apps
- Slow review process
APPLE DEVELOPER ENTERPRISE PROGRAM

- Requires **signing** with a special **enterprise certificate**
- An enterprise needs to **acquire** a certificate
- Program is for **internal** enterprise use only
- Apps can be published **directly** to Any iOS device from corporate server
- App is **not reviewed** by Apple
CASE SCENARIO

FORTUNE 100 COMPANY
~5,000 BYOD devices analyzed

RESULT WERE SURPRISING:
• 318 unique enterprise apps found
• 116 unique enterprise certificates were used
## CASE SCENARIO - FORTUNE 100 COMPANY

<table>
<thead>
<tr>
<th>Company Name</th>
<th>Partner Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>GOAPP SRL</td>
<td>Mobvantage Marketing Ltd.</td>
</tr>
<tr>
<td>MCE SYS LTD</td>
<td>GF Securities Co., Ltd.</td>
</tr>
<tr>
<td>Miracle Intelligent Network Co., Ltd.</td>
<td>Qingdao Qingqi Industry Co., Ltd.</td>
</tr>
<tr>
<td>QIAO BANG LIMITED</td>
<td>FitnessKeeper, Inc.</td>
</tr>
<tr>
<td>National Public Radio, Inc.</td>
<td>Dentsu McGarry Bowen LLC</td>
</tr>
<tr>
<td>Operator, Inc.</td>
<td>eVigilo Ltd.</td>
</tr>
<tr>
<td>Phind Corp.</td>
<td>Shanghai Yike Automation Technology Co., Ltd.</td>
</tr>
<tr>
<td>Proving Ground, LLC.</td>
<td>Humin Inc</td>
</tr>
<tr>
<td>Dropbox, Inc.</td>
<td>Hundsun Technologies Inc.,</td>
</tr>
<tr>
<td>Quooard Systems Limited</td>
<td>Shenzhen Sunline Tech Co., Ltd.</td>
</tr>
<tr>
<td>Huatai Securities Co., Ltd.</td>
<td>Shenzhen Baite Gifts Co., Ltd.</td>
</tr>
<tr>
<td>R/GA Media Group Inc.</td>
<td>Dongguan Chiting Trading Co., Ltd.</td>
</tr>
<tr>
<td>Readdle Inc.</td>
<td>Gameview sdn bhd</td>
</tr>
<tr>
<td>Reserve Media, Inc</td>
<td>Hangzhou HR Software Co., Ltd.</td>
</tr>
<tr>
<td>S.F. EXPRESS GROUP CO., LTD.</td>
<td>Fuzhou Yewen Advertising Co., Ltd.</td>
</tr>
<tr>
<td>Seasonal Spring LLC</td>
<td>Shanghai Soco Software Co., Ltd.</td>
</tr>
<tr>
<td>Shanghai Column Fashion Co., Ltd.</td>
<td>Shanghai 37 Degree Technology Co., Ltd.</td>
</tr>
</tbody>
</table>

Who can tell right from wrong?
NON APPSTORE CERTIFICATES

- whitelisted: 11
- Minimal reputation: 70
- No reputation: 33
- compromised: 2

- 72% Other
- 28% Asia
WHAT CAN ENTERPRISE APPS DO?

ABUSE PUBLIC APIs

- Microphone
- Location
- Address Book
- Calendar
- Pictures

ABUSE PUBLIC APIs

- Take Screenshot
- List Apps

EXPLOIT

- Jailbreak
- Masque
What **LIMITS** the enterprise app developer from doing all of those actions?
Trust

* And a user agreement
NO MALWARES

BECAUSE OF A USER AGREEMENT
ENTERPRISE CERTIFICATE ABUSE 3RD MARKET

- Third party App Stores use enterprise certificates to distribute apps.
- They often re-pack applications and distribute them.
- This is not a minor phenomenon

25PP – more than 40M users, 8M downloads a day in 2013

vShare – 40M users, 25% iOS. 15,000 iOS apps.
ENTERPRISE CERTIFICATE \textbf{ABUSE (2)}

- \textbf{FinFisher (2013)}
- \textbf{Masque Attack (2014)}
- \textbf{Hacking Team (2015)}
- \textbf{Pangu (2014)}
- \textbf{WireLurker (2015)}
- \textbf{YISpecter (2015)}
HACKING TEAM (1)

- Hacking Team got breached in July 2015
- iOS RAT source code was exposed
- Used an enterprise certificate to install malware
- Disguised as a newspaper in native Newsstand app
- Asks for extensive permissions
- Installs a key logger
- Leveraging masque attack
Hackers need location access even when the app is not in use.

- Location: Always
- Contacts: On
- Calendars: On
- Photos: On
- (void) startBackgroundSynch
{
    NSLog(@"Synch restarted!");

    dispatch_async(dispatch_get_global_queue(DISPATCH_QUEUE_PRIORITY_DEFAULT, 0), ^{
        while (self.jobExpired == NO)
        {
            [NSThread sleepForTimeInterval:gSynchDelay];

            gMainView = (ViewController*)[UIApplication sharedApplication].keyWindow.rootViewController;

            // Grab New Calendar and Contacts
            [gMainView getABContatcs];
            [gMainView getCalendars];

            [NSThread sleepForTimeInterval:1];

            // Synch to server
            [self performSync];
        }
    }

    @synchronized(self)
    {
        self.jobExpired = NO;
    }
}
LET'S TALK ABOUT MDMS

WHY ARE WE TALKING ABOUT MDM?

WAIT AND SEE
MOBILE DEVICE MANAGEMENT

Used by enterprises to support BYOD

- Deploy security policy
- Remote wipe
- Install applications
- Etc..
MOBILE DEVICE MANAGEMENT (2)

1. Wakeup request
2. Wakeup request
3. Status Request
4. Command

iOS Device

MDM Server

APNS

3. Status Request
4. Command
MOBILE DEVICE MANAGEMENT (2)

1. Wakeup request
2. Wakeup request
3. Status Request
4. Command

iOS Device
MDM Server
APNS
Install an iOS configuration profile:

- Can be used to route traffic through VPN/Proxy
- Can install root CA certificates
- Easy to deploy through phishing attacks
GOING BACK TO ENTERPRISE APPS
SECURITY FEATURES INTRODUCED IN iOS 9

- Apple understood the problem which lies in enterprise apps
- However, Enterprise apps cannot be eliminated
- Increase the complexity of executing enterprise apps
- Apps are cannot execute without explicit user trust
iOS <= 8

Hello Enterprise App!
iOS >= 9

Untrusted Enterprise Developer

Hello Enterprise App!
Enterprise uses MDM, Can’t do it to complicated..
BYPASSING THE GATEKEEPER

- Set up a remote enterprise app server
  - Serves the malicious enterprise app

- Initiate an MiTM attack
  - Wait for a command sent by the MDM server
  - Replace the command with an app install request
  - iOS device will fetch and install the enterprise app

- Enterprise app can now execute without explicit trust
  - User cannot tell the difference between enterprise and App Store app
ATTACK ANATOMY

iOS Device → Remote enterprise malicious app server

Wakeup request

APNS → MDM Server

Wakeup request
CONCLUSIONS

• Unverified code can be introduced to iOS ecosystem through Enterprise apps

• Non-jailbroken device are exposed to attacks

• Enterprises cannot trust the end user judgment in BYOD environments

• Enterprises should have a clear way to view and assess the enterprise app in their organizations

• MiTM attacks can be leveraged to gain access to a device
QUESTIONS?