RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

Challenge today's security thinking

SESSION ID: MBS-R01

Hackers Vs. The Anti-Malware Vendors: The Blue-Pill in Mobile Applications

Adi Sharabani

CEO & Co-Founder
Skycure

Yair Amit

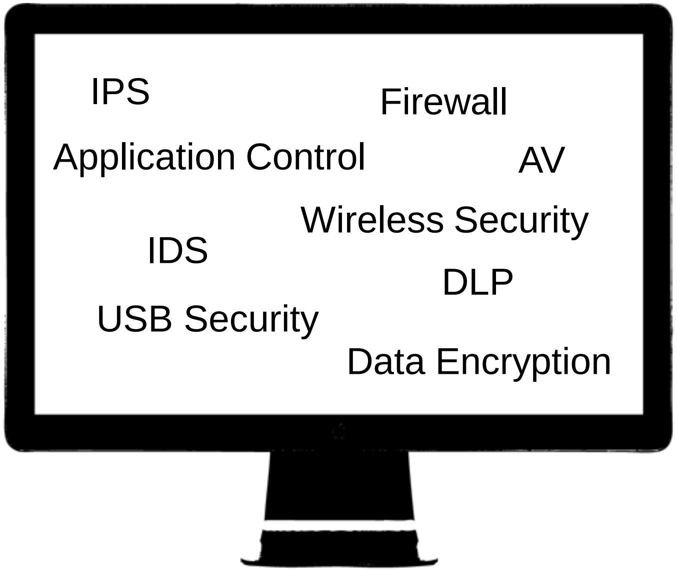
CTO & Co-Founder
Skycure

#RSAC

Agenda

- The Mobile Security Landscape
- Why, What, How of Malware
- Evolution of App Stores
- Popular Malware Detection Techniques
- Why They Fail
- Summary & Next Steps

Old Endpoint Vs. New Endpoint



IPS

Firewall

Application Control

AV

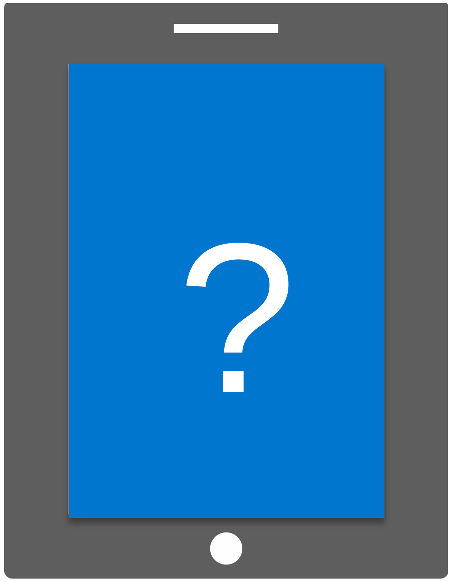
Wireless Security

IDS

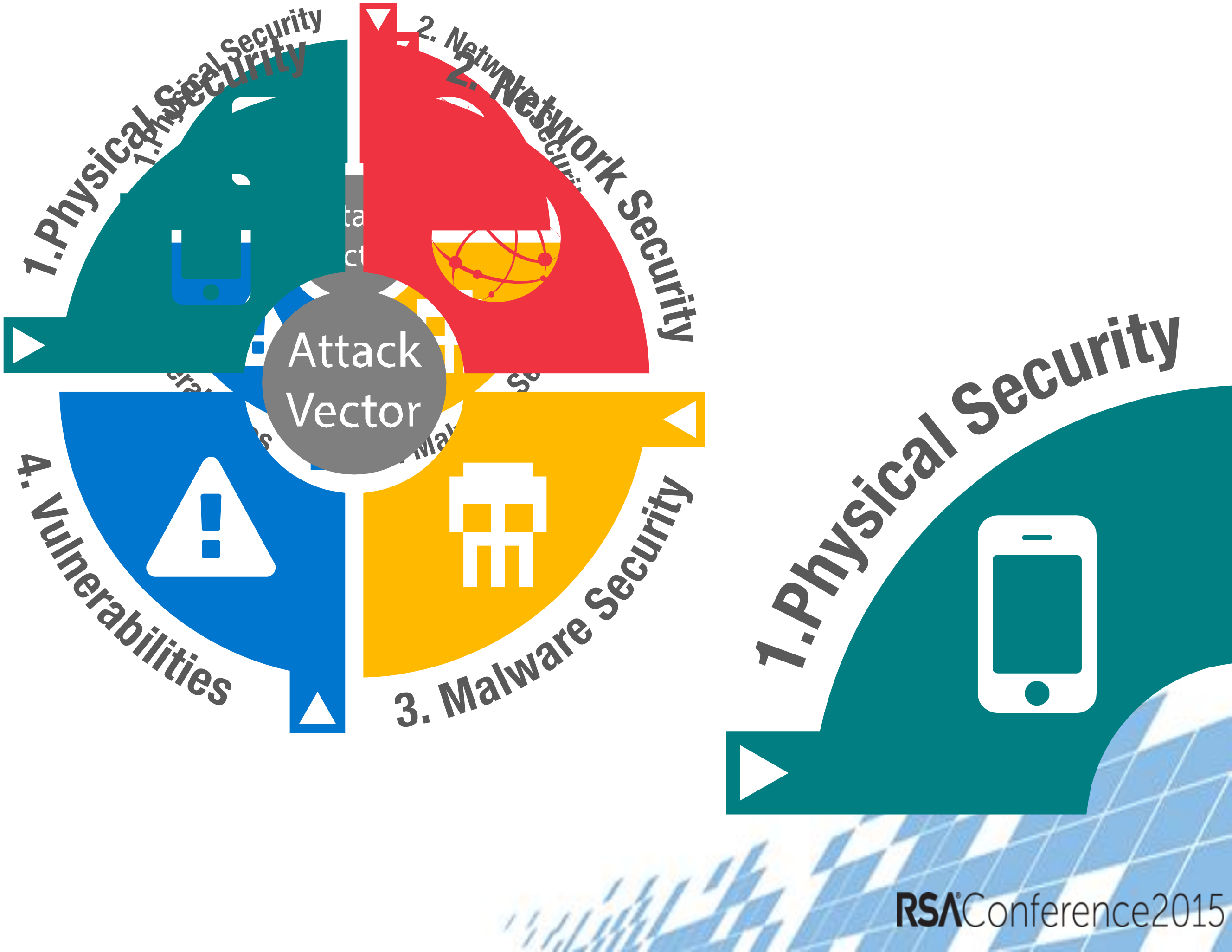
DLP

USB Security

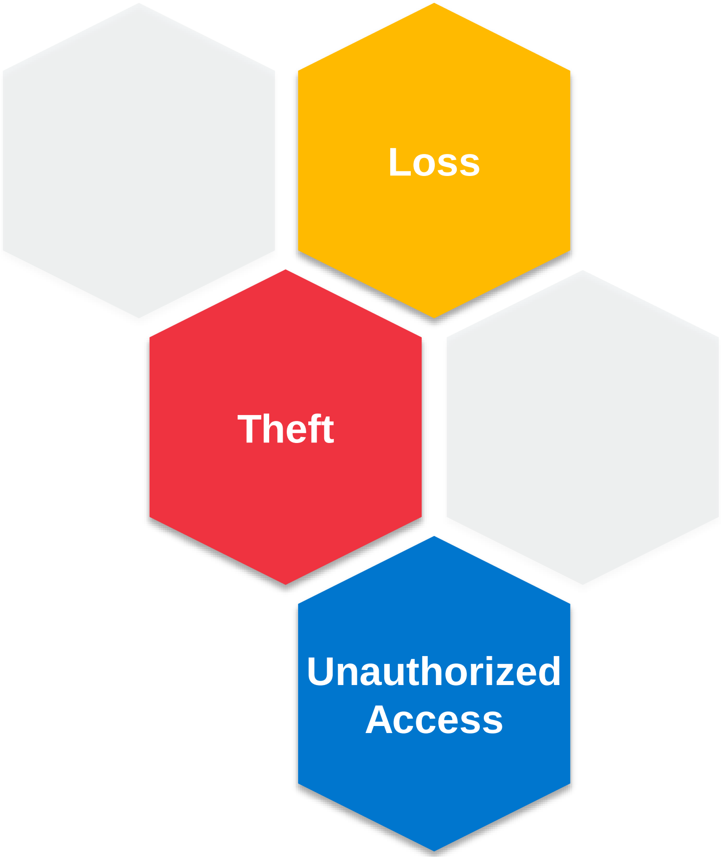
Data Encryption



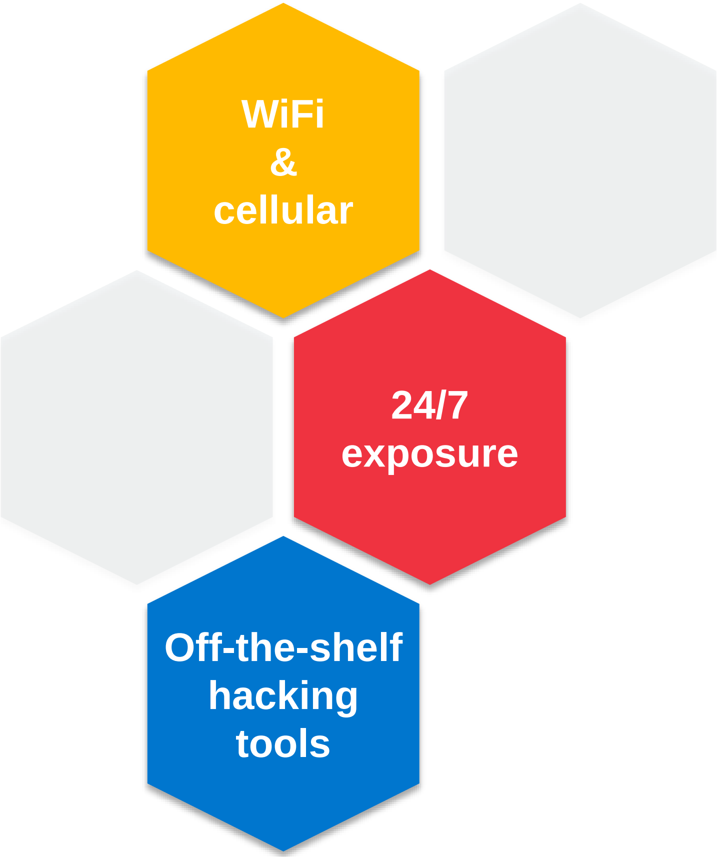
Modern Mobile Attacks



1.Physical Security



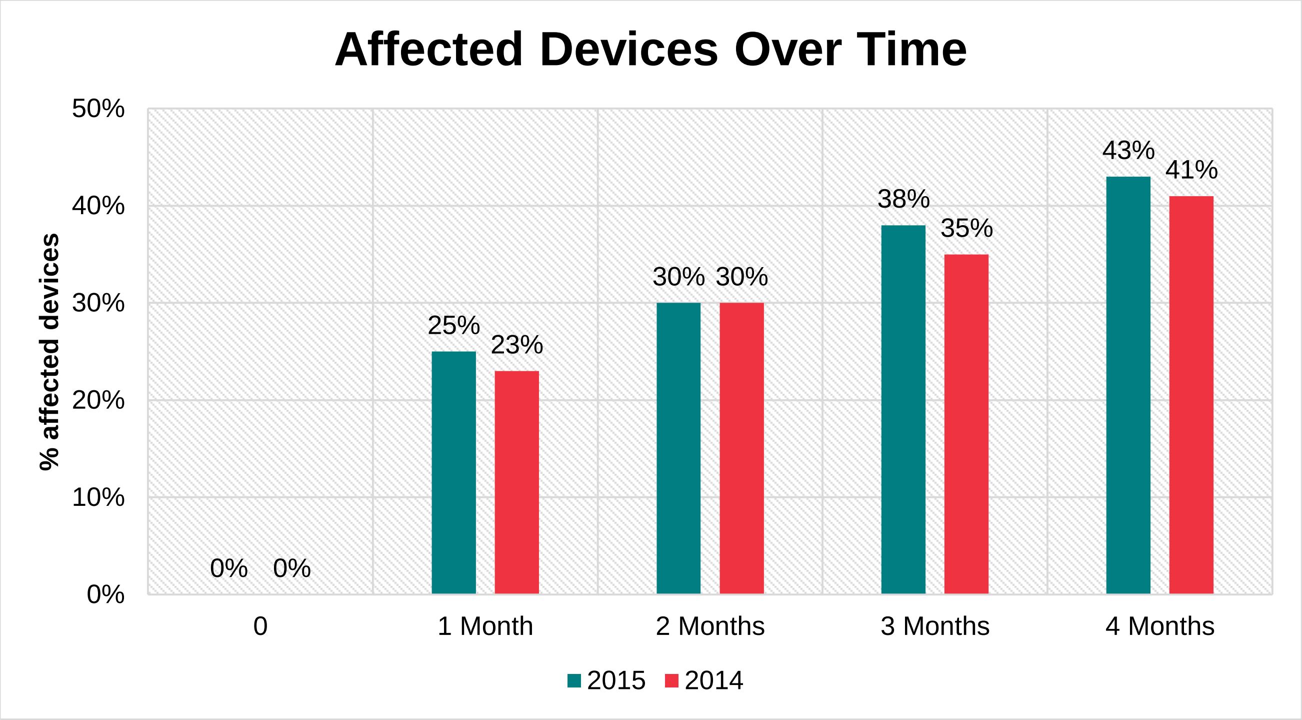
2. Network Security



WiFi & cellular

24/7 exposure

Off-the-shelf hacking tools



Based on Skycure Threat Intelligence

2. Network Security

Skycure

RSAConference2015

3. Malware Security

External Android stores

Repackaged apps

iOS impact

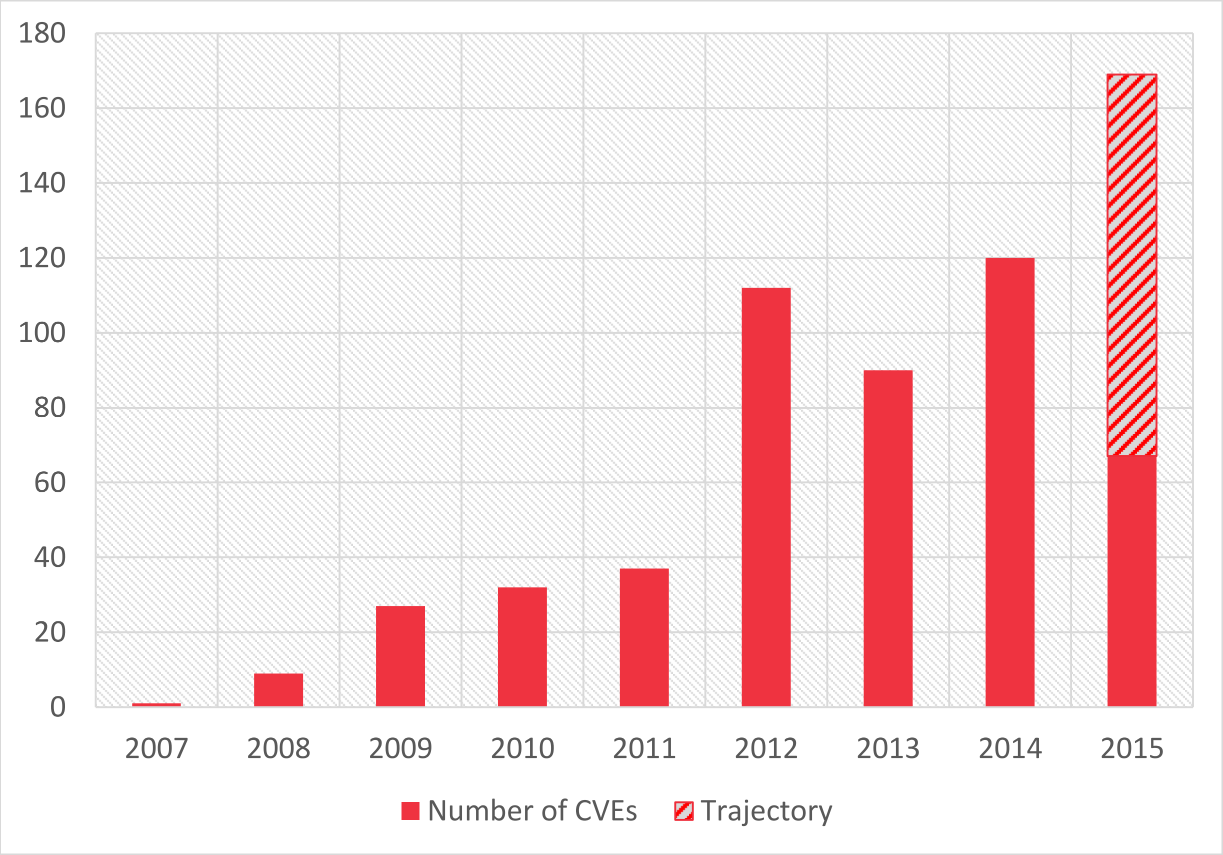
4. Vulnerabilities

OS & app-level

Patching challenges

Never-ending story

4. Vulnerabilities



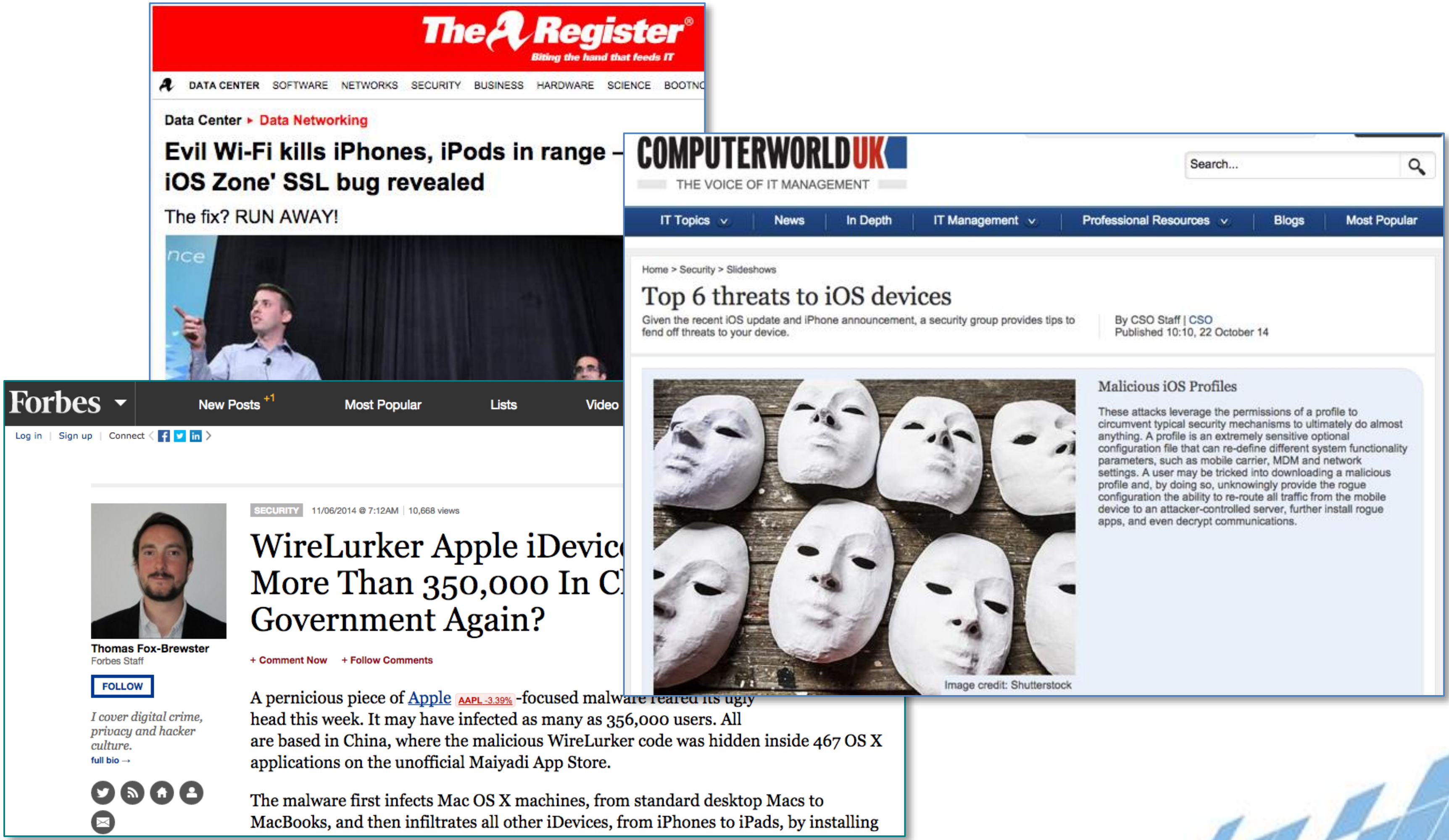
Source: Skycure analysis based of CVEdetails.com

Let’s talk Mobile Malware

VENOM

E708 CCN

Malware is Not Just an Android Problem



The Register®
Biting the hand that feeds IT

DATA CENTER SOFTWARE NETWORKS SECURITY BUSINESS HARDWARE SCIENCE BOOTNO

Data Center ▸ Data Networking

Evil Wi-Fi kills iPhones, iPods in range – iOS Zone' SSL bug revealed

The fix? RUN AWAY!

Forbes

New Posts +1
Most Popular
Lists
Video
Log in | Sign up | Connect

SECURITY 11/06/2014 @ 7:12AM | 10,668 views

WireLurker Apple iDevic More Than 350,000 In C Government Again?

Thomas Fox-Brewster
Forbes Staff

I cover digital crime, privacy and hacker culture.
full bio →

+ Comment Now + Follow Comments

A pernicious piece of Apple AAPL -3.39% -focused malware reared its ugly head this week. It may have infected as many as 356,000 users. All are based in China, where the malicious WireLurker code was hidden inside 467 OS X applications on the unofficial Maiyadi App Store.

The malware first infects Mac OS X machines, from standard desktop Macs to MacBooks, and then infiltrates all other iDevices, from iPhones to iPads, by installing

COMPUTERWORLDUK
THE VOICE OF IT MANAGEMENT

Home > Security > Slideshows

Top 6 threats to iOS devices

Given the recent iOS update and iPhone announcement, a security group provides tips to fend off threats to your device.

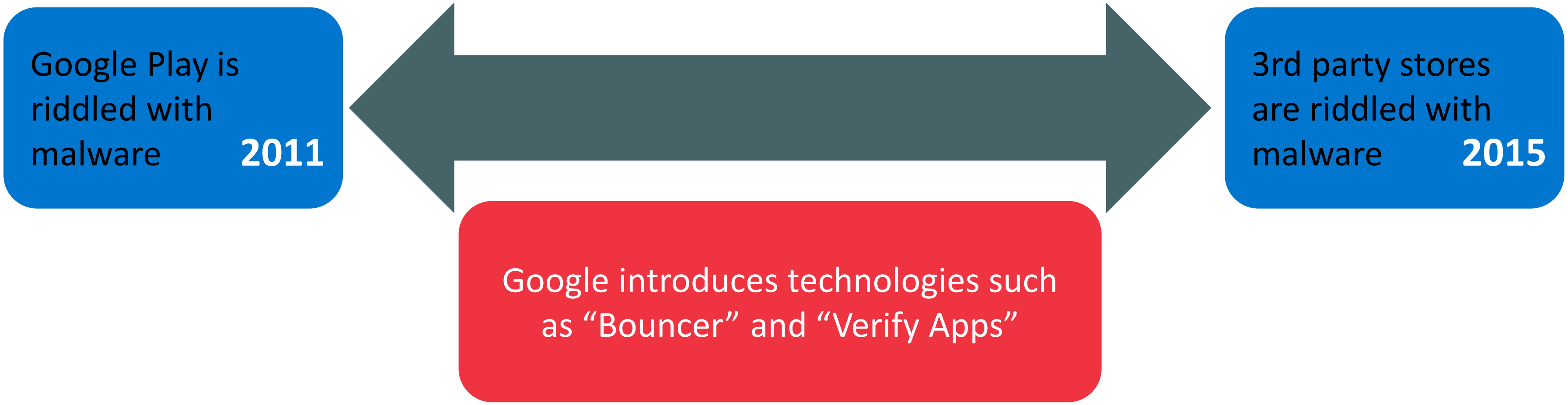
By CSO Staff | CSO
Published 10:10, 22 October 14

Malicious iOS Profiles

These attacks leverage the permissions of a profile to circumvent typical security mechanisms to ultimately do almost anything. A profile is an extremely sensitive optional configuration file that can re-define different system functionality parameters, such as mobile carrier, MDM and network settings. A user may be tricked into downloading a malicious profile and, by doing so, unknowingly provide the rogue configuration the ability to re-route all traffic from the mobile device to an attacker-controlled server, further install rogue apps, and even decrypt communications.

Image credit: Shutterstock

Evolution of Android Malware

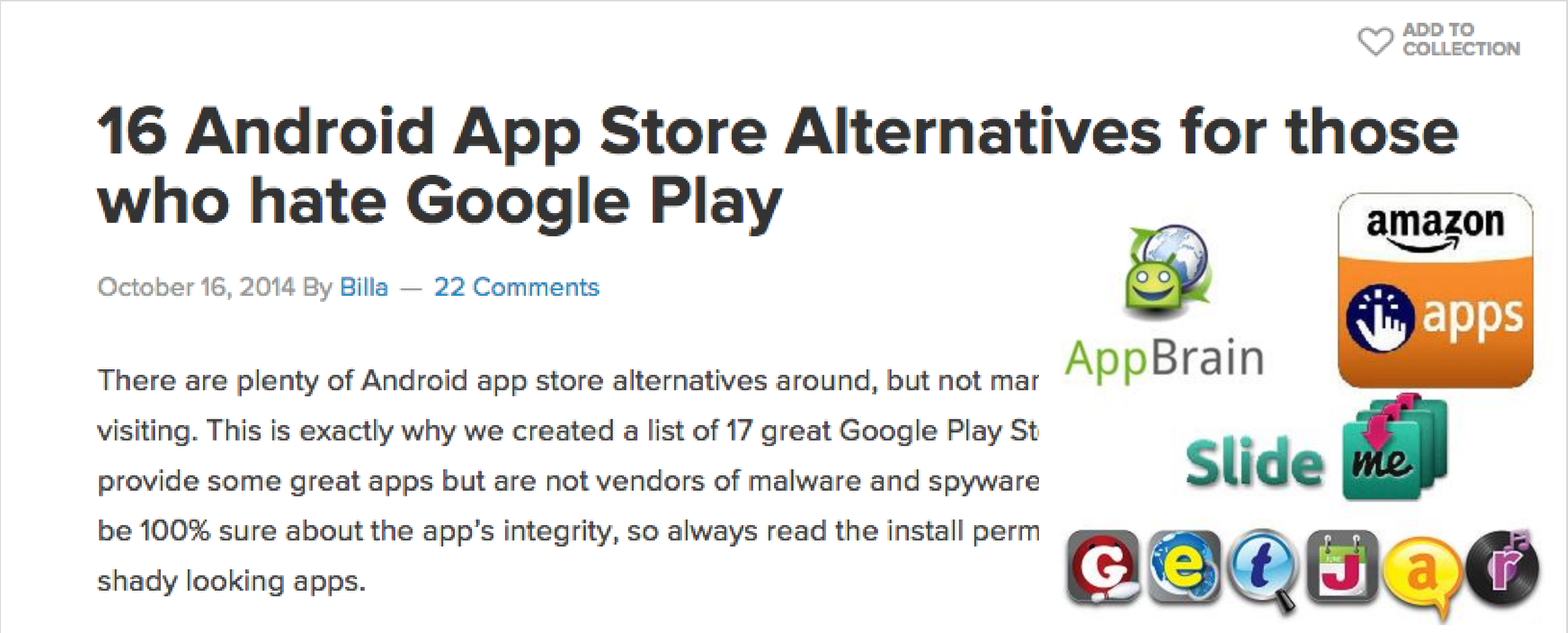


Google Play is riddled with malware **2011**

3rd party stores are riddled with malware **2015**

Google introduces technologies such as “Bouncer” and “Verify Apps”

Third-Party App Stores



16 Android App Store Alternatives for those who hate Google Play

October 16, 2014 By Billa — 22 Comments

There are plenty of Android app store alternatives around, but not mar visiting. This is exactly why we created a list of 17 great Google Play St provide some great apps but are not vendors of malware and spyware be 100% sure about the app's integrity, so always read the install perm shady looking apps.

Popular Malware Detection Techniques

Signature-based

+	−
Simple, Low FP, High TP.	Evasion, Zero-Day, Limited.

Static Analysis

+	−
Fast, Easy, Cheap.	FP/FN, Run-time, Limited.

Dynamic Analysis

+	−
No code, Any app, Run-time	FP/FN, Fix time, Limited.

Bypassing Static Analysis

- Dynamic code loading from a remote website
- Reflection

We will share a few code snippets and analyze them with the audience to show how they trick current static analysis technology.

Bypassing Dynamic Analysis

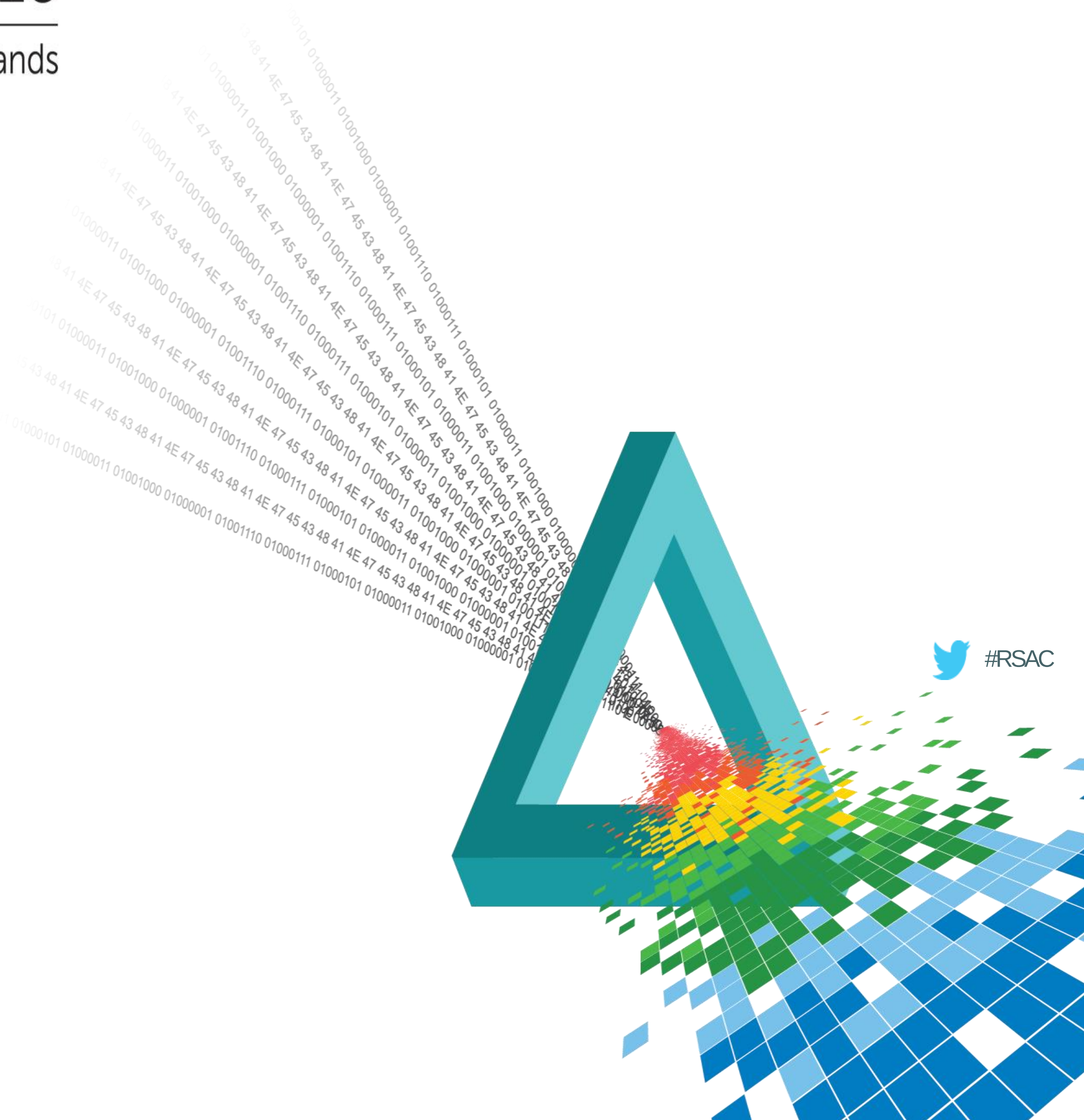
- Time bombs
- Am I running in a debugger? [Anti debugging]
- Response from the server decides if to go by the “bad path”

Benign Apps Behave in a Similar Manner

- Main reasons:
  - IP protection
  - Security by obscurity
- Techniques:
  - Dynamic code loading
  - Anti debugging
  - ProGuard

RSAConference2015

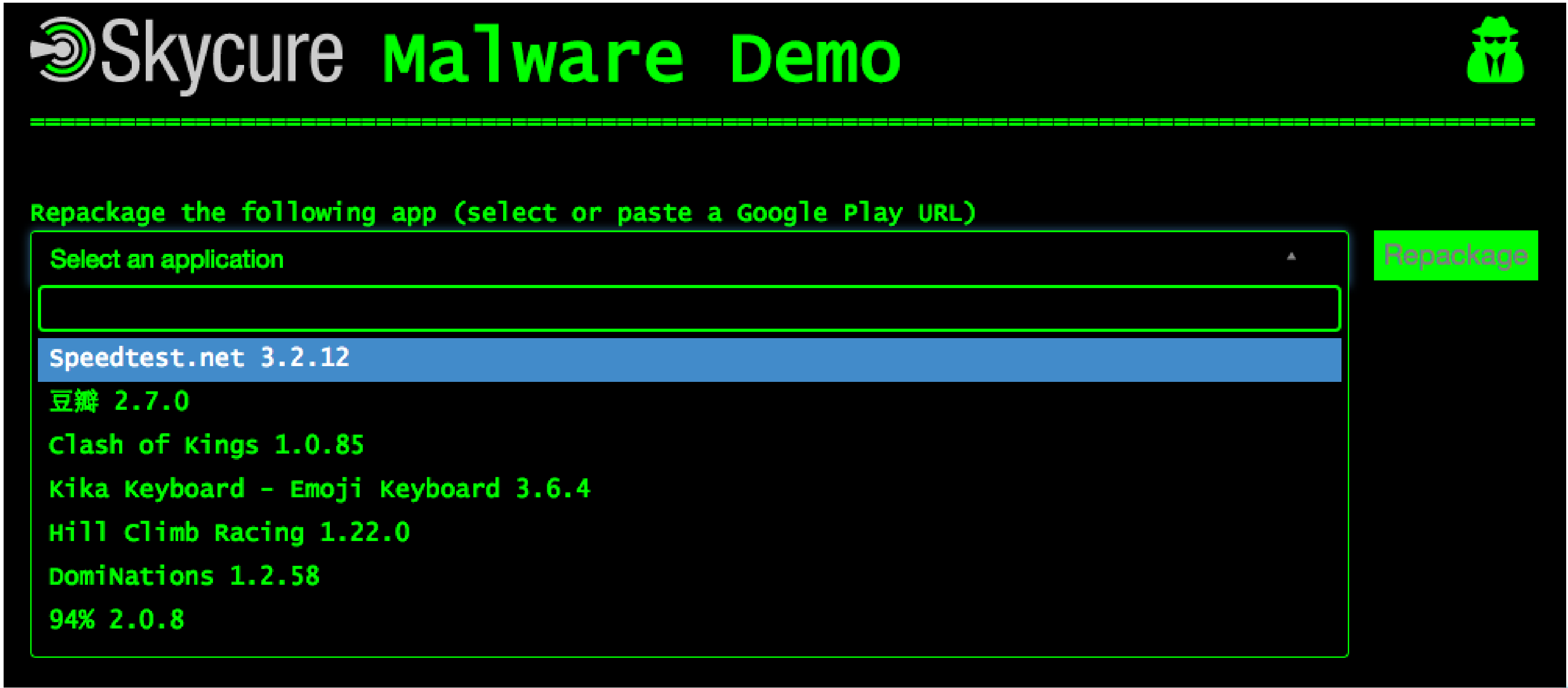
Singapore | 22-24 July | Marina Bay Sands



#RSAC

Android Demo

Repackaged Apps



Skycure **Malware Demo**

Repackage the following app (select or paste a Google Play URL)

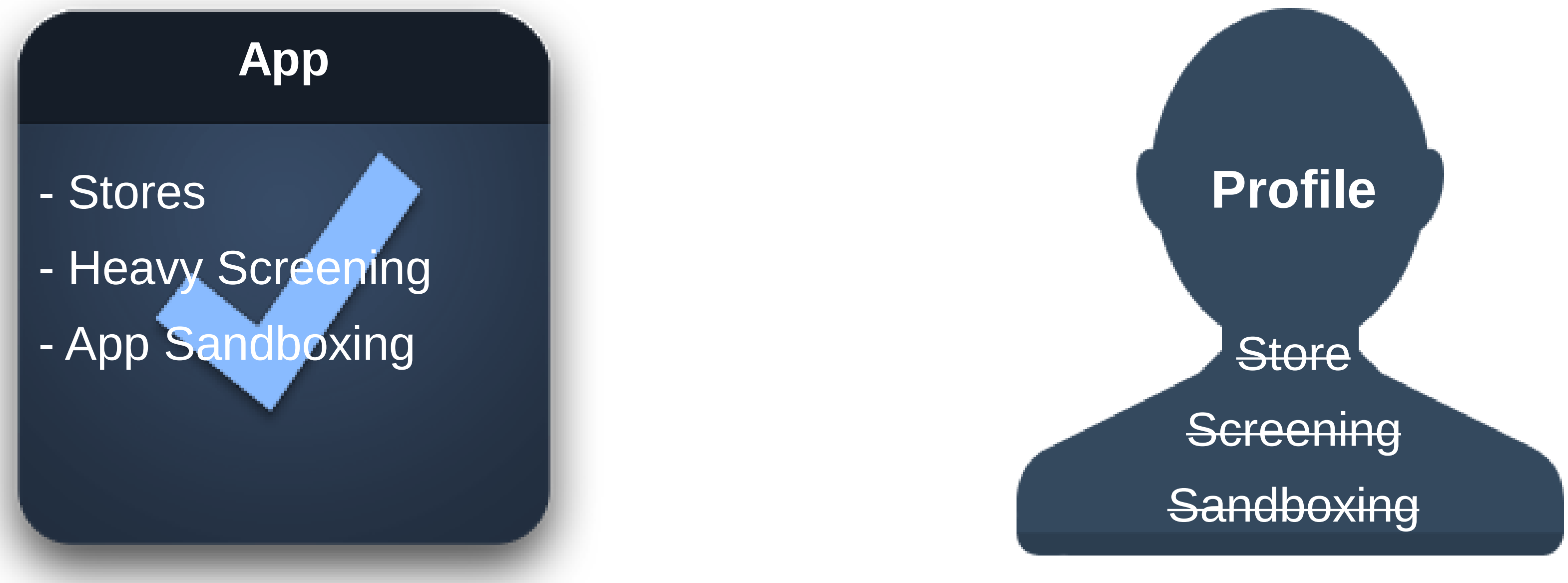
Select an application

- Speedtest.net 3.2.12
- 豆瓣 2.7.0
- Clash of Kings 1.0.85
- Kika Keyboard - Emoji Keyboard 3.6.4
- Hill Climb Racing 1.22.0
- DomiNations 1.2.58
- 94% 2.0.8

To remove infection, please delete the app!

What About iOS?

- Can malware solutions catch Malicious Profiles?



App

- Stores

- Heavy Screening

- App Sandboxing

Profile

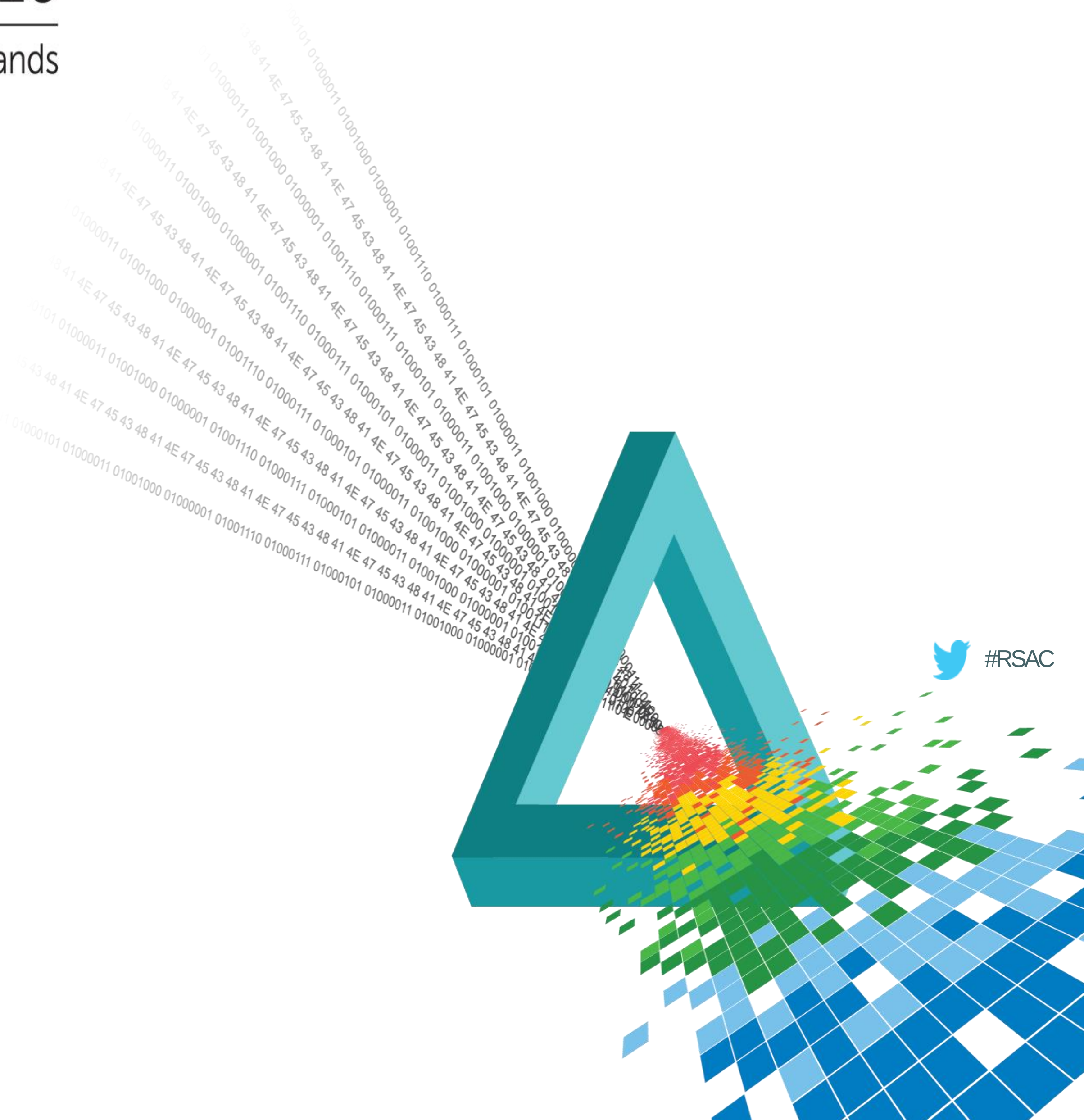
~~Store~~

~~Screening~~

~~Sandboxing~~

RSAConference2015

Singapore | 22-24 July | Marina Bay Sands



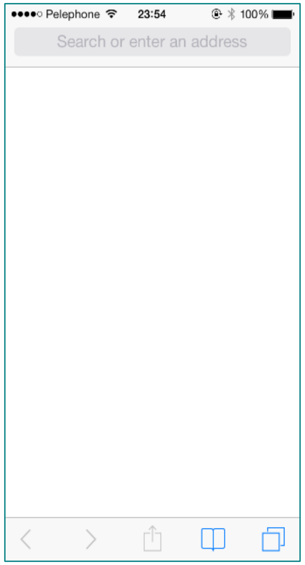
#RSAC

iOS Demo

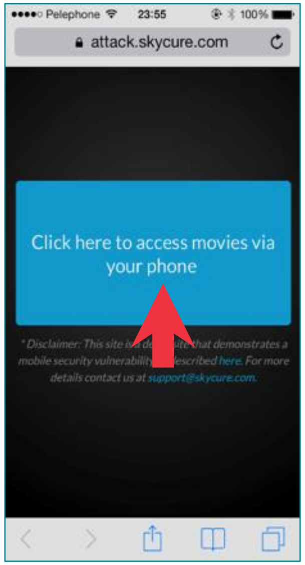
Participation Instructions

Start demo by opening Safari and browsing to:

attack.skycure.net

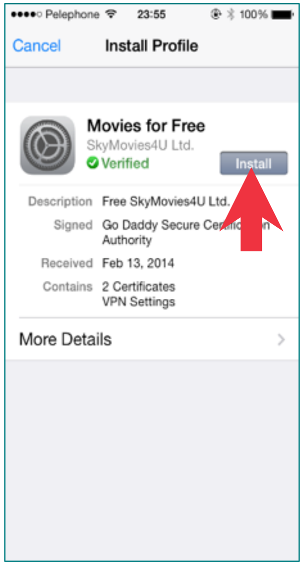


1. Open your Safari


●●●●○ Pelephone 23:55 100%
attack.skycure.com
Click here to access movies via your phone

*Disclaimer: This site is a de[illegible] site that demonstrates a mobile security vulnerability [illegible] described here. For more details contact us at support@skycure.com.

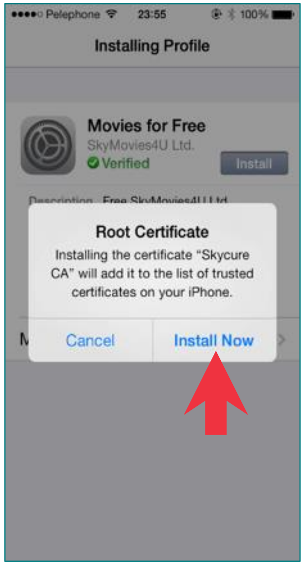
2. Tap the blue button



Movies for Free
SkyMovies4U Ltd.
✓ Verified

Description: Free SkyMovies4U Ltd.
Signed: Go Daddy Secure Certification Authority
Received: Feb 13, 2014
Contains: 2 Certificates, VPN Settings

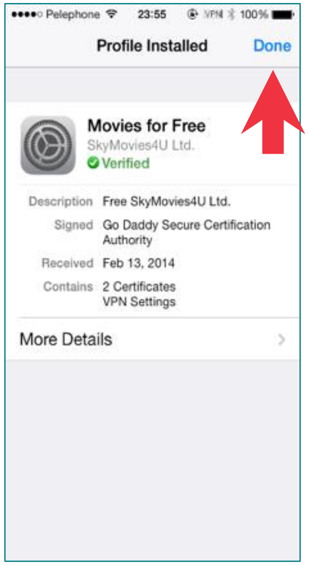
3. Click on 'Install'



Root Certificate

Installing the certificate "Skycure CA" will add it to the list of trusted certificates on your iPhone.

4. Click on 'Install Now'

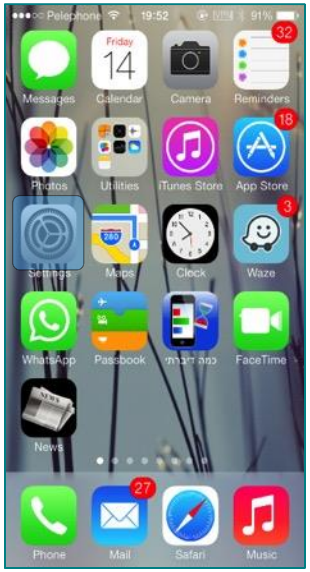


Movies for Free
SkyMovies4U Ltd.
✓ Verified

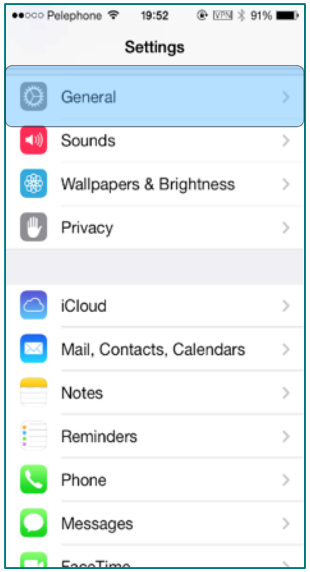
Description: Free SkyMovies4U Ltd.
Signed: Go Daddy Secure Certification Authority
Received: Feb 13, 2014
Contains: 2 Certificates, VPN Settings

5. Click on 'Done'

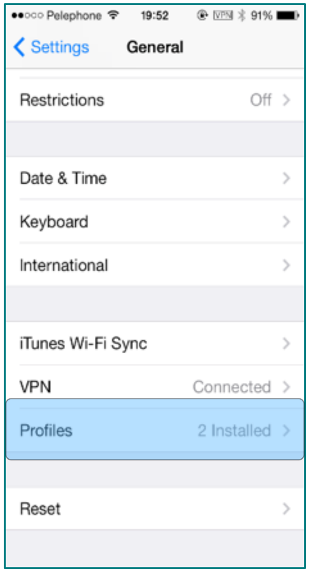
Removing The Infection



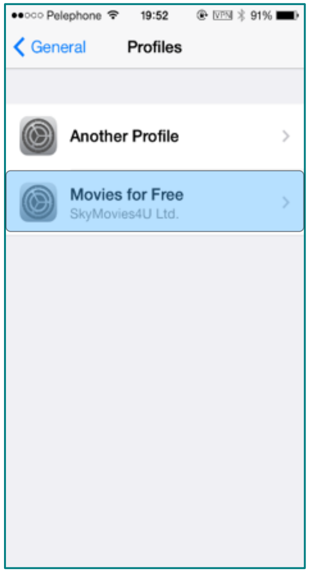
1. Go to Settings



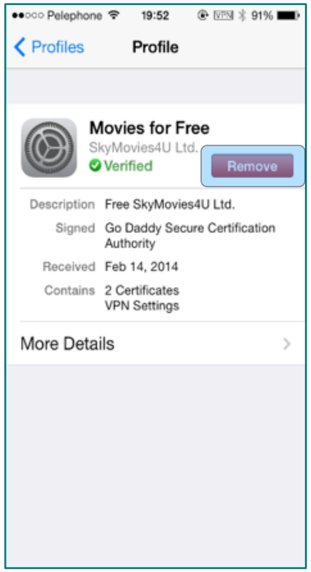
2. Click on General



3. Click on Profiles



4. Click on “Movies for Free”



Movies for Free
SkyMovies4U Ltd.
✓ Verified

Description Free SkyMovies4U Ltd.
Signed Go Daddy Secure Certification Authority
Received Feb 14, 2014
Contains 2 Certificates
VPN Settings

5. Click on Remove

Try again with Skycure installed on your device.

Available on the App Store

ANDROID APP ON Google play

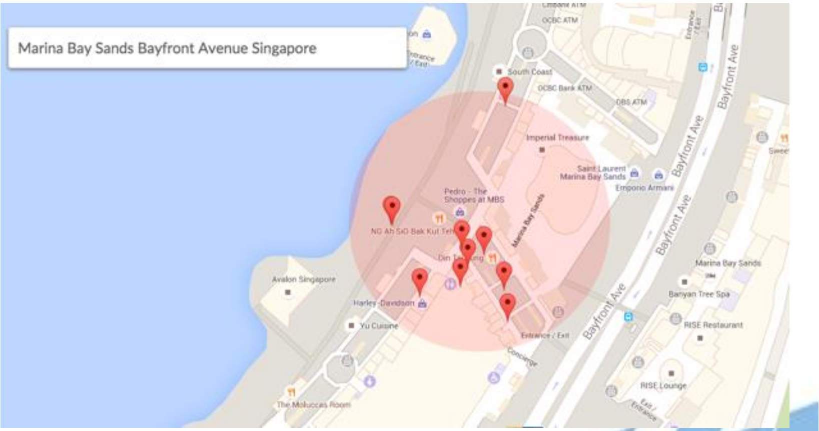
Skycure

RSAConference2015

Do They Always Need Malware?

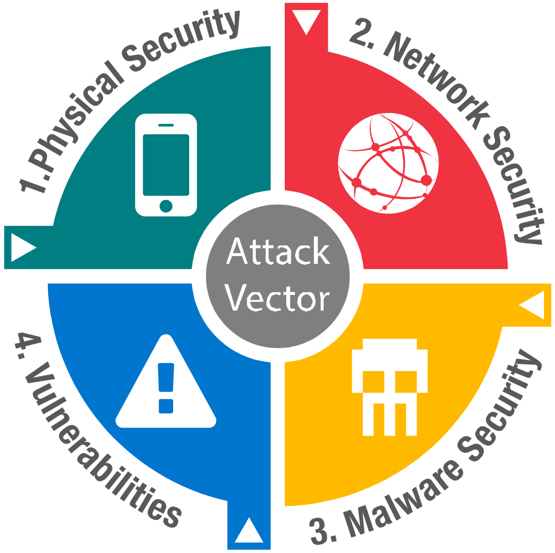
“No-iOS Zone” Attack

- iOS users in range are unable to use their mobile devices
  - No WiFi, no offline work, no phone calls, no airplane mode…
- Potential areas that may be attractive for attackers:
  - Political events
  - Wall Street
  - Economical & business events
  - Governmental and military facilities
  - Marina Bay Sands?



Summary

- Malware is becoming more sophisticated
- Classical anti-malware approaches struggle with detection and protection
- Malware is only one element of the mobile threat landscape



Apply What You Have Learned

- Gain visibility into all mobile attacks
- Protect beyond malware
- Use more than static and dynamic analysis
  - Reputation-based Analysis
  - Signature-based Analysis
  - Application Permission Analysis
  - Static Analysis
  - Dynamic Analysis
  - Crowd Intelligence (https://maps.skycure.com)

Q&A And Next Steps

✉ contact@skycure.com

https://www.skycure.com

https://blog.skycure.com

@SkycureSecurity, @AdiSharabani, @YairAmit

/Skycure