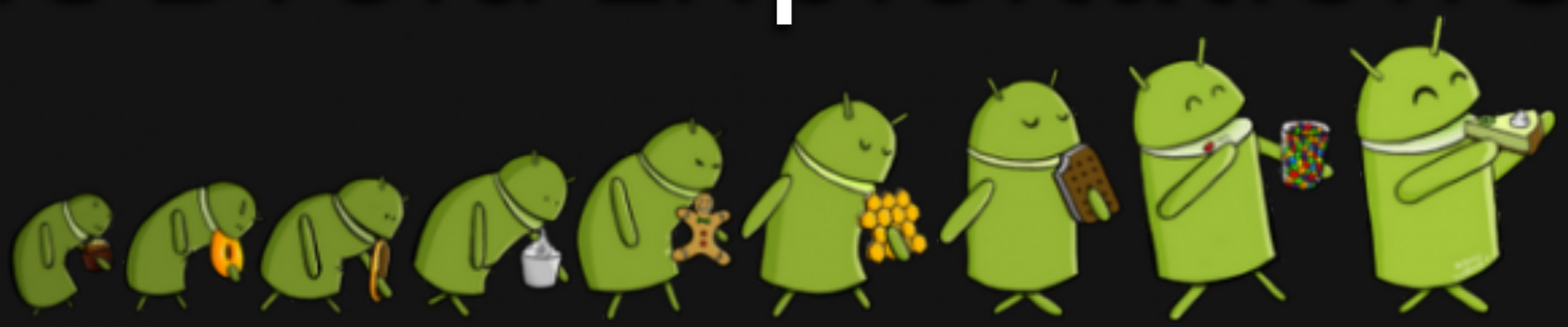
black hat ABU DHABI 2012
DECEMBER 10 – 13, 2012
EMIRATES PALACE | UNITED ARAB EMIRATES
In partnership with:
TRA
KHALIFA UNIVERSITY
Supported by:
aeCERT

The Droid Exploitation Saga



Subho Halder | @sunnyrockzzs

Aditya Gupta | @adi1391

XY Security Consultancy Services

Who are we !

- Information security researcher
- Mobile exploiter
- creator of afe (android framework for exploitation)
- python lovers
- co-founder of xysec.
- found bug in some famous websites including Google, Apple, Microsoft, Skype, Adobe and many more

XY Security
Consultancy Services

SOME COMPANIES WE'VE FOUND VULNS IN..

Microsoft

facebook

Adobe

PayPal™ YAHOO! skype™

tumblr.

rediff.com

STANFORD UNIVERSITY

And MORE...

Agenda

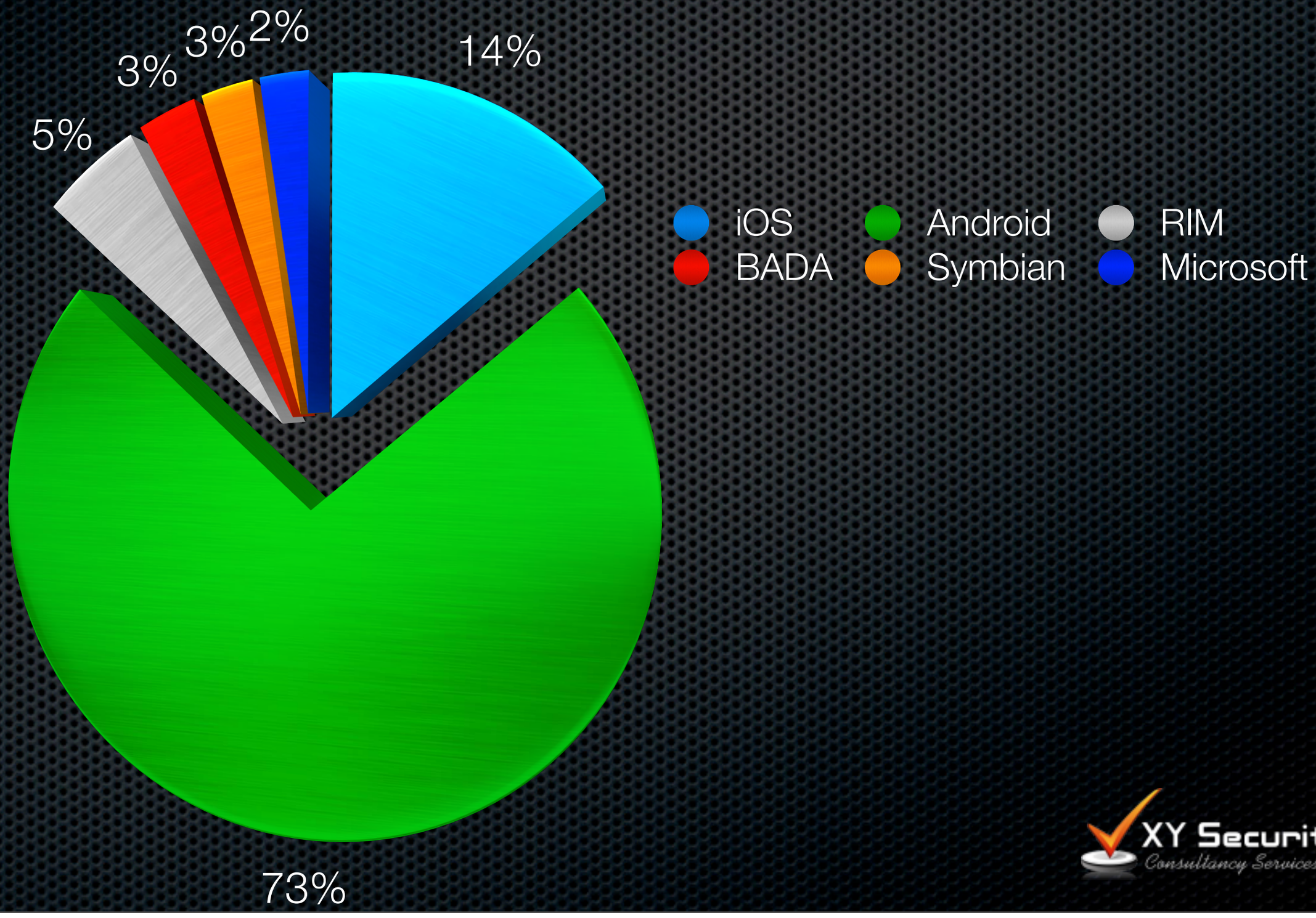
- Quick Intro to Android
- Android Security Model
- Creating Android malwares
- Android Botnets
- Injecting malwares into another app
- Content Providers
- Creating own modules for AFE
- Fuzzing, Penetration Testing with AFE

Android

- Open-sourced platform by Google Inc
- Generic builds, which can be deployed in any Hardware Configuration.
- Linux Kernel, Webkit Browser, Open-Sourced Applications

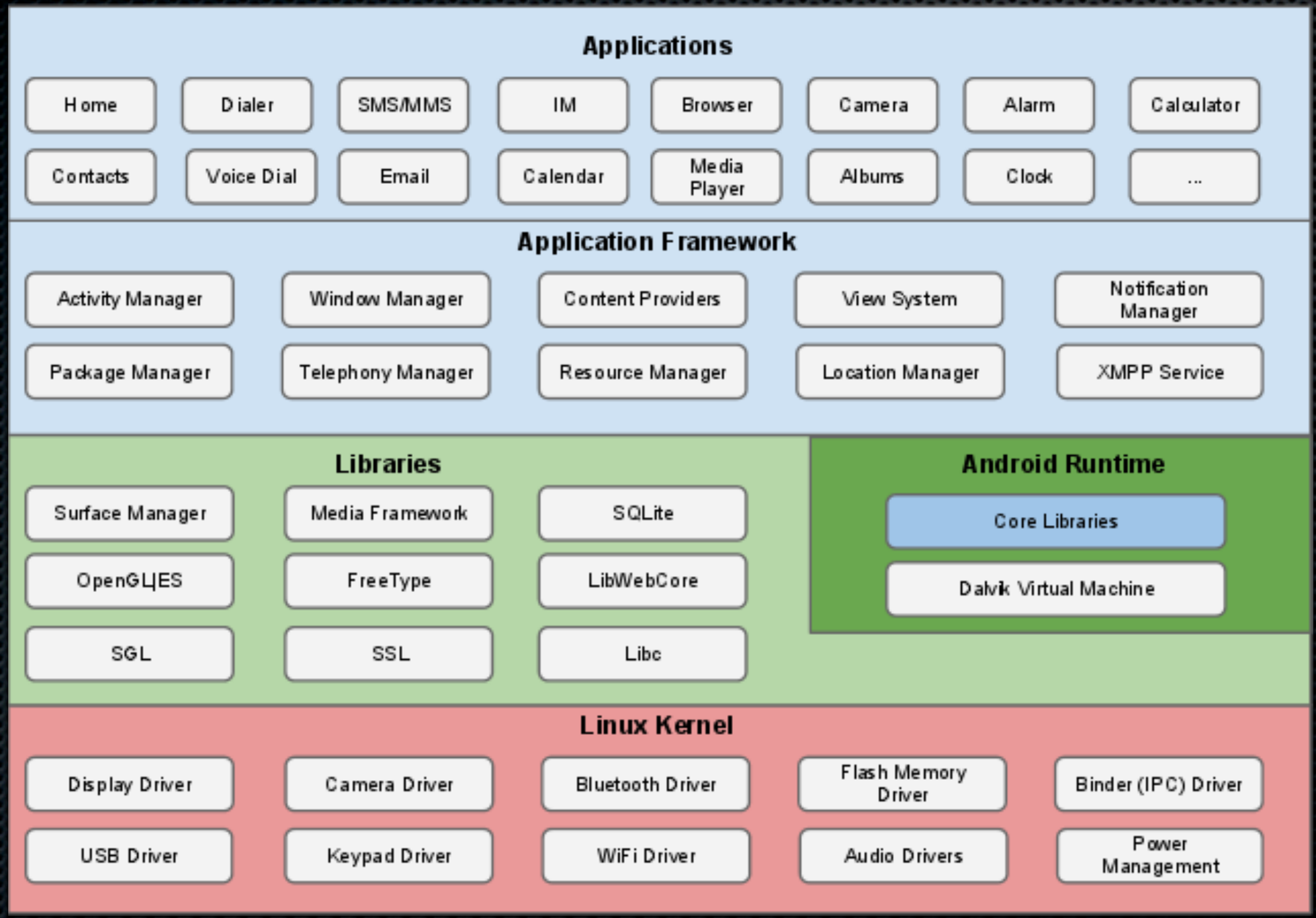
XY Security
Consultancy Services

Market Share



XY Security
Consultancy Services

Android Architecture



Android Applications

- Written mainly in Java+little XML
- Composed of components:
  - Activities
  - Services
  - Intents
  - Content Providers
  - Broadcast Receivers

XY Security
Consultancy Services

Security Architecture

- Apps run in a virtual env/sandbox
- Privilege Separation
- Each app has its own UID n GID
- ASLR in most places (from >4.0)
- DVM
- IPC - Inter Process Communication
- Dalvik VM != Sandbox

XY Security
Consultancy Services

Security Architecture

```
# ps
USER     PID   PPID  VSIZE  RSS     WCHAN    PC         NAME
root      1     0     368    220   c0077dc0 000090cc S /init
root      2     0     0      0     c009015c 00000000 S kthreadd
root      3     2     0      0     c007aeec 00000000 S ksoftirqd/0
root      4     2     0      0     c00aeac4 00000000 S watchdog/0
root      5     2     0      0     c008c214 00000000 S events/0
```

```
system    19682 1304  135620 15020 ffffffff ffff0520 S com.sec.android.providers.drm
app_78    19770 1304  146072 23376 ffffffff afd0c5bc S com.whatsapp
radio     19788 1304  138720 20488 ffffffff afd0c5bc S com.wssyncmldm
app_41    19807 1304  135888 16740 ffffffff afd0c5bc S com.sec.android.widgetapp.dualclock
app_39    19816 1304  157876 23580 ffffffff afd0c5bc S com.google.android.apps.maps:GoogleLocat
```

XY Security
Consultancy Services

Permission Model

- Defined in **AndroidManifest.xml**
- Displayed to user when installing the app
- Not exactly a XML file
- Defines the package name, version name, min SDK level required and the permission

```
<uses-sdk android:minSdkVersion="10" />

<application
    android:icon="@drawable/ic_launcher"
    android:label="@string/app_name" >
    <activity
        android:name=".GpsTutorialActivity"
        android:label="@string/app_name" >
        <intent-filter>
            <action android:name="android.intent.action.MAIN" />

            <category android:name="android.intent.category.LAUNCHER" />
        </intent-filter>
    </activity>
</application>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
    <uses-permission android:name="android.permission.INTERNET" />
```

XY Security Consultancy Services

Which one?

- An app with just **INTERNET** permission
- An app asking for **ALL** permissions
- An app asking for **READ_LOGS** permission
- An app asking for **0** permission

Bypassing the permission model

INTERNET

Use Browser, upload using GET

ACESS FILES FROM SDCARD

No Permission Needed !

JUICY INFORMATION

Use READ_LOGS

XY Security
Consultancy Services

Content Providers

- A content provider manages access to a central repository of data.
- The provider is part of an Android application, which often provides its own UI for working with the data.
- A content provider is identified by a content URI.

Accessing a Content Provider

- Example of getting a list of words from the User Dictionary provider:

```
// Queries the user dictionary and returns results
mCursor = getContentResolver().query(
    UserDictionary.Words.CONTENT_URI,   // The content URI of the words table
    mProjection,                        // The columns to return for each row
    mSelectionClause                    // Selection criteria
    mSelectionArgs,                     // Selection criteria
    mSortOrder);                        // The sort order for the returned rows
```

- The content URI of the words table is: content://user_dictionary/words

- Read permission for accessing the content provider is also needed in the manifest file:

```
<uses-permission android:name="android.permission.READ_USER_DICTIONARY">
```

XY Security Consultancy Services

```
<provider android:authorities="list"
          android:enabled=["true" | "false"]
          android:exported=["true" | "false"]
          android:grantUriPermissions=["true" | "false"]
          android:icon="drawable resource"
          android:initOrder="integer"
          android:label="string resource"
          android:multiprocess=["true" | "false"]
          android:name="string"
          android:permission="string"
          android:process="string"
          android:readPermission="string"
          android:syncable=["true" | "false"]
          android:writePermission="string" >
    . . .
</provider>
```

Content Providers

XY Security
Consultancy Services

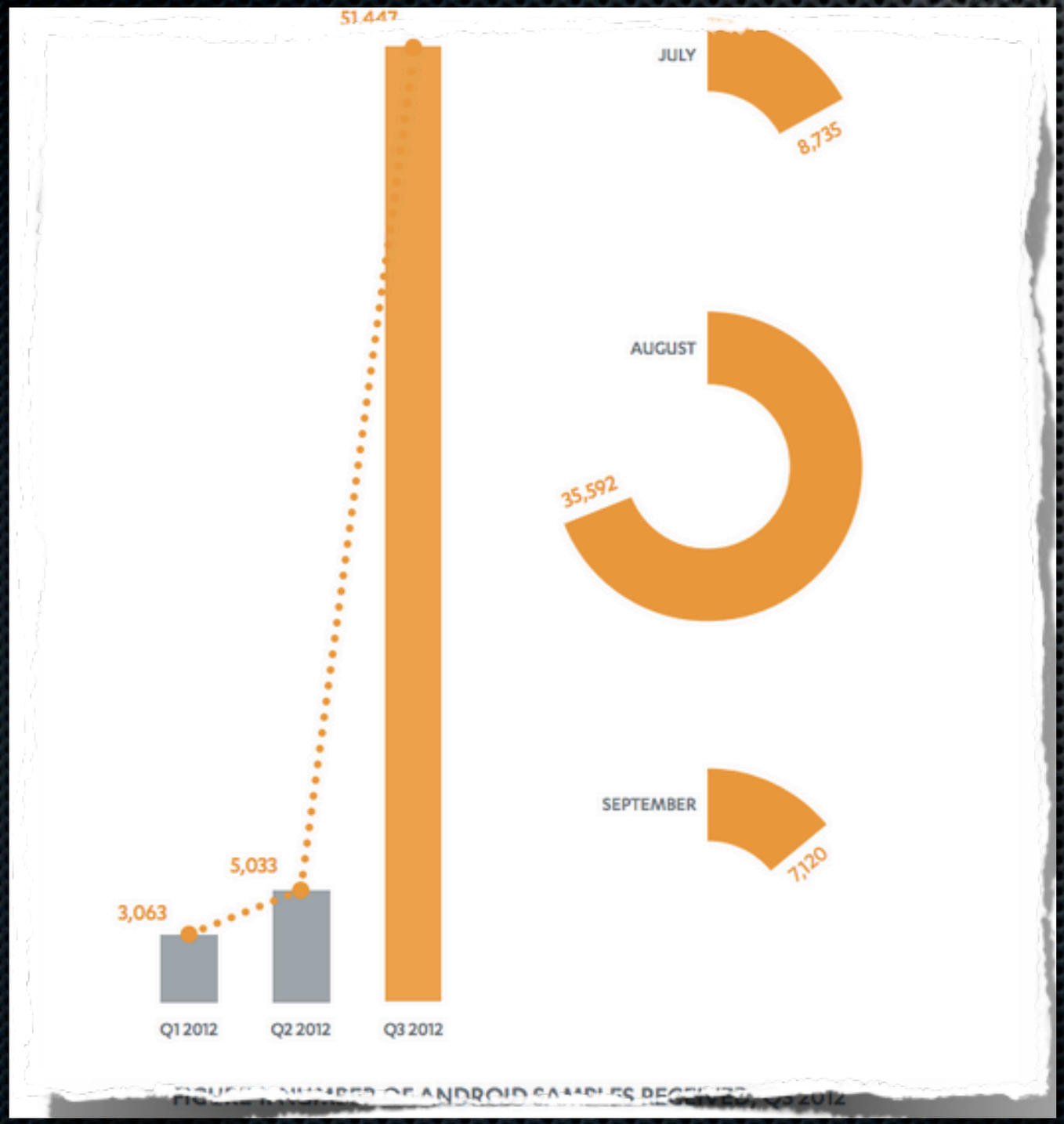
What about Google Bouncer!

- Virtual Environment to check if a particular app is malicious
- Runs the app in a phone/environment before publishing to the market
- Detects most of the malwares

XY Security
Consultancy Services

HOT TOPICS NOMINATE FOR THE CRUNCHIES APPLE FACEBOOK AMAZON TWITTER GOOGLE

Android Malware Surges Despite Google's Efforts To Bounce Dodgy Apps Off Its Platform; F-Secure IDs 51,447 "Unique Samples" In Q3



source: Fsecure

XY Security Consultancy Services

Android Malwares (common features)

- Send SMS to premium numbers
- Subscribe to premium services
- Dial premium numbers
- Steal messages, contact list, call logs
- Steal SD Card files
- Autorespond to text messages with some predefined format

Creating a malware

- Use **Content Providers** to get all the information
- **Cursors** & **SQLite** Databases
- Write Java codes like crazy
- Send that data to remote server using **HTTP**
- Set up a **PHP** file to listen to incoming data
- Save it to a **SQL** Database

XY Security
Consultancy Services

How can you Automate these?

XY Security
Consultancy Services

XY Security
Consultancy Services

AFE Internals

Plugin Based Architecure

Modules

Python Based

Libraries

XY Security
Consultancy Services

AFE Perspective

Offensive	Defensive
Malware Creation	Content Query
BotNet Automation	App Assesment
Crypting	Fuzzing
Injecting	Kernel Assessment

XY Security
Consultancy Services

Creating Malwares/Botnets

```
Set Reverse IP
Change APP Name
Stealer
Build it !
Upload malformed APK
Back
```

```
Set your reverse IP, you can either start the listener and listen
or send data to your own server by providing full path including http://
```

```
Steal Call Logs only
Steal SMS Inbox only
Steal Contacts only
Steal Call Logs and SMS
Steal Call Logs and Contacts
Steal SMS and Contacts
Steal all
```

```
Build Completed in 6 seconds. Find the created apk in /output folder
```

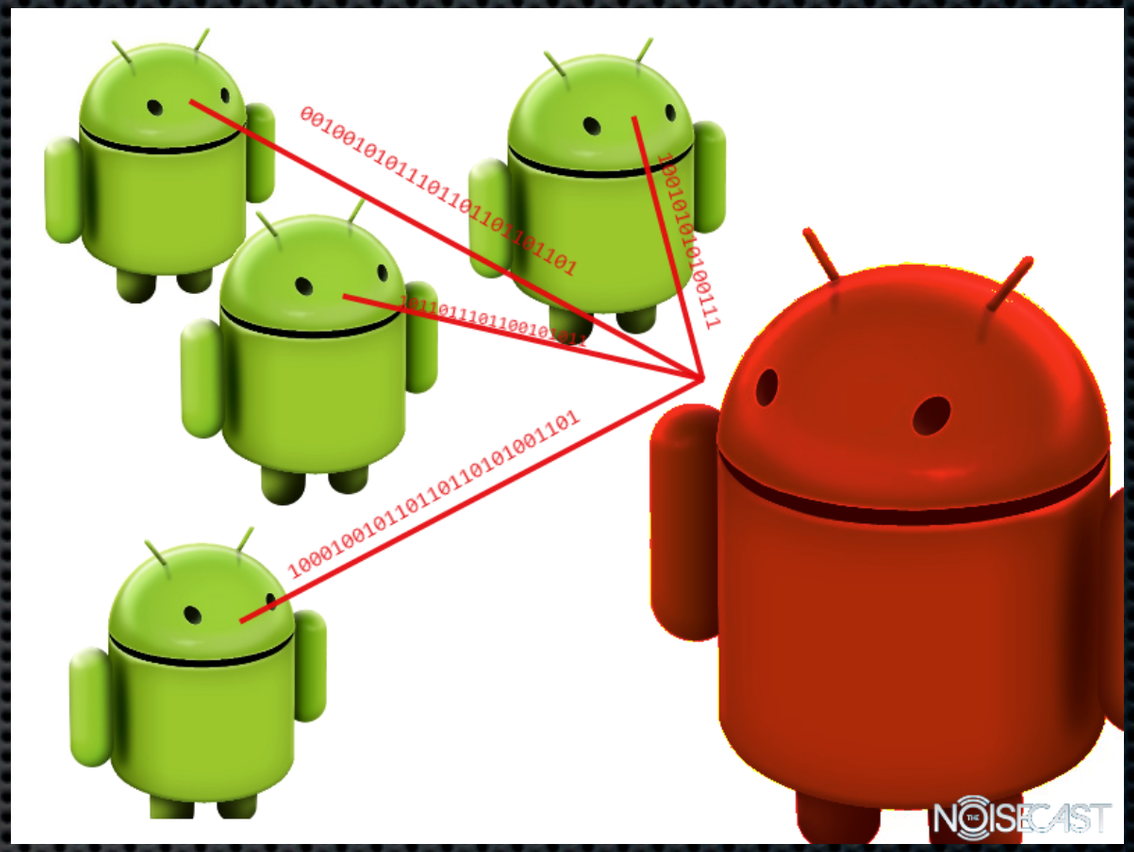
XY Security
Consultancy Services

DEMO

(MALWARES WITH AFE)

XY Security
Consultancy Services

Botnets



- More popular in PCs
- Gradually coming to mobile
- Already seen some cases
- Harder to detect in mobile phones
- AVs not effeceint
- C & C easier in PCs

XY Security
Consultancy Services

Botnets

- Can be used to get reverse shell + all malware features
- C & C over ~~HTTP~~ SMS
- Battery consumption increases suspiciously with HTTP
- Can even execute shell commands with SMS
- Get the output as an SMS
- No notification on the victim’s phone

XY Security
Consultancy Services

Botnets

- Operated all over just SMS
- No need of r00t
- Incoming messages won’t show a notification
- Identify each slave with its unique ID
- Remote Shell `xysec cat /proc/version`
- Further exploitation
- Botnet = $$$

XY Security
Consultancy Services

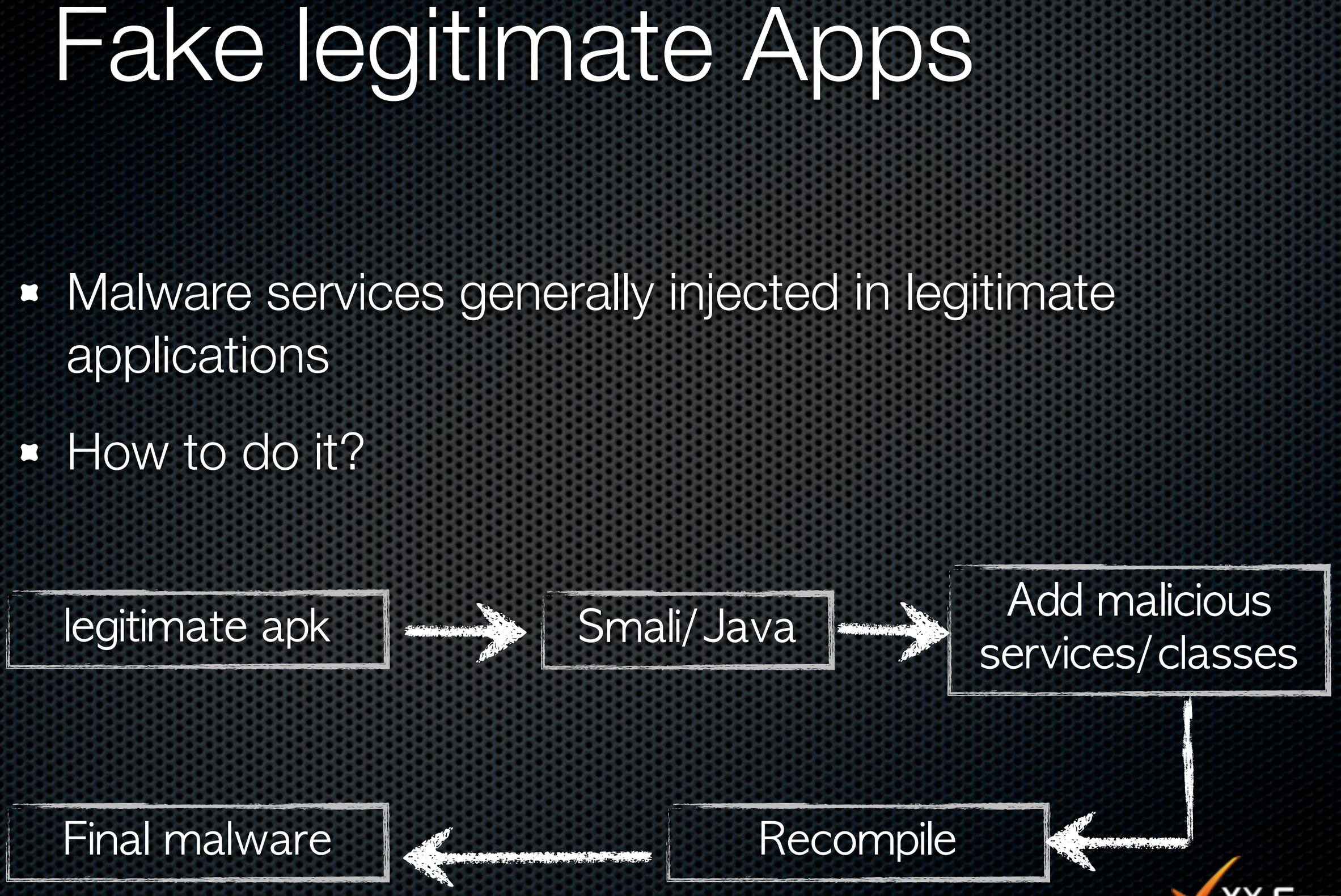
DEMO

(BOTNETS WITH AFE)

XY Security
Consultancy Services

Fake legitimate Apps

- Malware services generally injected in legitimate applications
- How to do it?

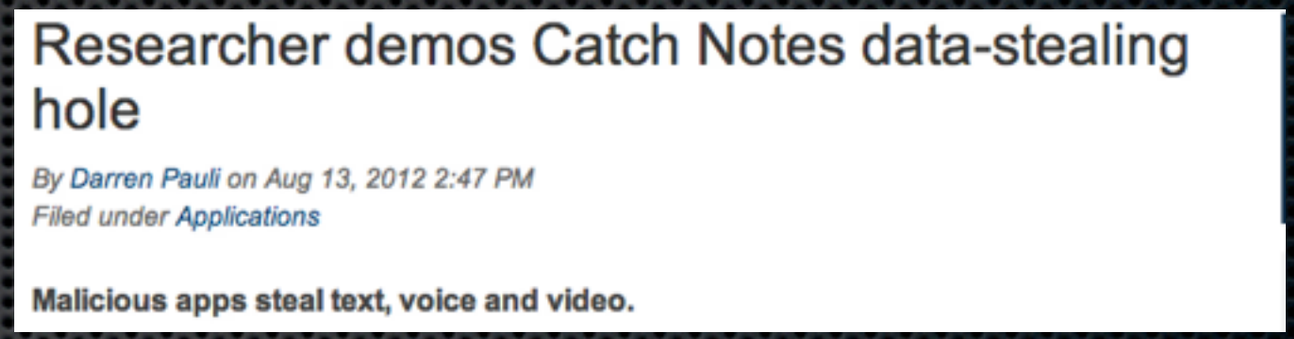


XY Security
Consultancy Services

Or Use AFE

Stealing Content Providers

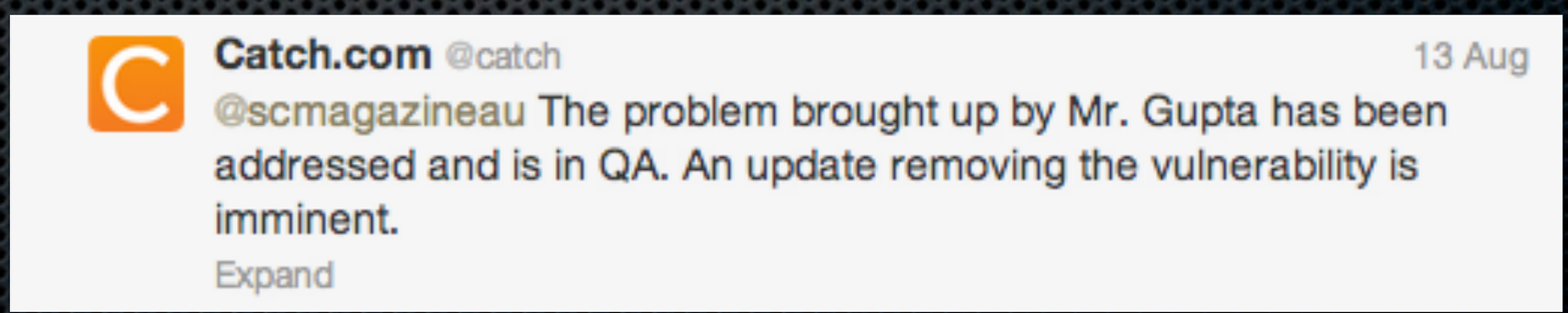
- Catch application
- Over a million downloads
- Saves its notes using vuln content provider
- POC



Researcher demos Catch Notes data-stealing hole

By Darren Pauli on Aug 13, 2012 2:47 PM
Filed under Applications

Malicious apps steal text, voice and video.



Catch.com @catch 13 Aug

@scmagazineau The problem brought up by Mr. Gupta has been addressed and is in QA. An update removing the vulnerability is imminent.

Expand

XY Security Consultancy Services

Bypassing the anti malwares

XY Security
Consultancy Services

Bypassing the anti malwares

Matches the signature with its database

XY Security
Consultancy Services

Bypassing the anti malwares

Matches the signature with its database

Checks the activity, service and other class names

XY Security
Consultancy Services

Bypassing the anti malwares

Matches the signature with its database

Checks the activity, service and other class names

checks the names of the variables

XY Security
Consultancy Services

Bypassing the anti malwares

Matches the signature with its database

Checks the activity, service and other class names

checks the names of the variables

Checks the control flow graph

XY Security
Consultancy Services

Matches the signature with its database

Rebuild + Zipalign

Checks the activity, service and other class names

checks the names of the variables

Checks the control flow graph

XY Security
Consultancy Services

Matches the signature with its database

Checks the activity, service and other class names

checks the names of the variables

Checks the control flow graph

Modifies the classnames and all its references within files

XY Security
Consultancy Services

Matches the signature with its database

Checks the activity, service and other class names

checks the names of the variables

Checks the control flow graph

Split variables into two, and append at runtime

XY Security
Consultancy Services

Matches the signature with its database

Checks the activity, service and other class names

checks the names of the variables

Checks the control flow graph

Add dummy loops to change CFG

XY Security
Consultancy Services

Early Detection

virustotal

SHA256:	718910c7d9ebab4d6a19b7f1be64b6ca7978920ae1c01e6e37dff30b017d7221
File name:	file-4832922_apk
Detection ratio:	30 / 46
Analysis date:	2012-12-03 18:52:50 UTC (1 day, 11 hours ago)

More details

XY Security
Consultancy Services

After Crypting

virustotal

SHA256:	b4dc06304259198a361c180d36b5bfc85c36e4dd10b4cae06f20c3780eeddc99
SHA1:	5ea259c8e1bad5c67c0947e671559d95177ece36
MD5:	9e40e3b02f4e664390c7c6ab3f4022c0
File size:	68.4 KB (69992 bytes)
File name:	1-stringcrypt.apk
File type:	Android
Detection ratio:	4 / 46
Analysis date:	2012-12-05 05:29:29 UTC (0 minutes ago)

Less details

XY Security
Consultancy Services

Checking your apps for vulnerabilities

- Find out leaky content providers
- How to find content providers a particular app is using? (use AFE)
- Try extracting the contents of that Content Provider using another app (use AFE)
- Insecure file storage (use your brain)
- Insecure data transmission (Use Proxy)
- Authentication + Other problems

XY Security
Consultancy Services

Being secure

- Use obfuscators such as ProGuard (uses Name obfuscation, optimization, CFG obfuscation) or Dasho
- Check before you publish
- Have your “USB Debugging” turned OFF
- Don’t rely on AV
- Too paranoid? Reverse before you use. :)

QUESTIONS?

security@xysec.com
http://afe-framework.com
https://github.com/xysec/AFE