LEAKING ADS – IS USER DATA TRULY SECURE?

Roman Unuchek

Security Researcher
Kaspersky Lab
FINDINGS

- 4 million apks exposing data
- Device information, user information, GPS coordinates
- Advertising SDK’s
THE BEGINNING

- List of installed apps
- GCM ID
- Personal information (DOB, name, gender..)
- App usage
- GPS coordinates
THE BEGINNING

- Device information
- Personal information (age, gender)
- GPS coordinates
My own Device

- Device information
- Network information
- Token for push messages
- GPS coordinates
SDKs

3rd party code in APPs

- 25%
- 20%
- 10%
Since 2014, more than 4 years!

- 13,622,391 APK files
- 131,203,322 unique URLs
- 14,906,467 PCAP files
GET

POST
### TOP URLs

<table>
<thead>
<tr>
<th>URL</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>mopub.com</td>
<td>apps.ad-x.co.uk</td>
</tr>
<tr>
<td>rayjump.com</td>
<td>typany.com</td>
</tr>
<tr>
<td>9apps.com</td>
<td>mobpowertech.com</td>
</tr>
<tr>
<td>advertise.1mobile.com</td>
<td>api.zephyr-digital.com</td>
</tr>
<tr>
<td>applovin.com</td>
<td>salmonads.com</td>
</tr>
<tr>
<td>tapas.net</td>
<td>lds.lenovomm.com</td>
</tr>
<tr>
<td>appsgeyser.com</td>
<td>afric.wocao.in</td>
</tr>
<tr>
<td>appioapp.com</td>
<td>config.cloudzad.com</td>
</tr>
<tr>
<td>taobao.com</td>
<td>m.mobogenie.com</td>
</tr>
<tr>
<td>duapps.com</td>
<td>cabinet.taximaxim.ru</td>
</tr>
</tbody>
</table>
mopub.com

- &dn=samsung,GT-I9300,m0xx
- &w=320&h=480
- &mcc=624&mnc=1
- &bundle=com.some.app
- &q=gender:m,age:27
- &ll=47.6144939,-122.1964071

Mitigation: do not provide user data to 3rd parties
<table>
<thead>
<tr>
<th></th>
<th>Updated</th>
<th>Size</th>
<th>Installs</th>
<th>Requires Android</th>
<th>Installs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>January 30, 2018</td>
<td>Varies with device</td>
<td>100,000,000 - 500,000,000</td>
<td>4.1 and up</td>
<td>50,000,000 - 100,000,000</td>
</tr>
<tr>
<td></td>
<td>January 10, 2018</td>
<td>Varies with device</td>
<td>100,000,000 - 500,000,000</td>
<td></td>
<td>10,000,000 - 50,000,000</td>
</tr>
<tr>
<td></td>
<td>December 15, 2017</td>
<td>Varies with device</td>
<td>100,000,000 - 500,000,000</td>
<td></td>
<td>5,000,000 - 10,000,000</td>
</tr>
<tr>
<td></td>
<td>January 10, 2018</td>
<td>Varies with device</td>
<td>100,000,000 - 500,000,000</td>
<td></td>
<td>1,000,000 - 5,000,000</td>
</tr>
<tr>
<td></td>
<td>January 28, 2018</td>
<td>Varies with device</td>
<td>100,000,000 - 500,000,000</td>
<td></td>
<td>500,000 - 1,000,000</td>
</tr>
</tbody>
</table>
rayjump.com

- `platform=1&os_version=4.1.2`  
  [device info]
- `model=GT-I9300&brand=Samsung`  
  [device info]
- `screen_size=320x480`  
  [device info]
- `mnc=1&mcc=250&network_type=1`  
  [network info]
- `package_name=com.some.app`  
  [app name]
- Mitigation: limit permissions
<table>
<thead>
<tr>
<th>Updated</th>
<th>Installs</th>
<th>Current Version</th>
<th>Updated</th>
<th>Installs</th>
<th>Requires Android</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 7, 2018</td>
<td>500,000,000 - 1,000,000,000</td>
<td>4.0.28_ww</td>
<td>February 7, 2018</td>
<td>100,000,000 - 500,000,000</td>
<td>4.0.3 and up</td>
</tr>
<tr>
<td>February 6, 2018</td>
<td>Varies with device</td>
<td></td>
<td>February 8, 2018</td>
<td>500,000,000 - 1,000,000,000</td>
<td></td>
</tr>
<tr>
<td>January 28, 2018</td>
<td>100,000,000 -</td>
<td></td>
<td>January 23, 2018</td>
<td>Varies with device</td>
<td></td>
</tr>
<tr>
<td>January 31, 2018</td>
<td>Varies with device</td>
<td></td>
<td>February 8, 2018</td>
<td>100,000,000 - 500,000,000</td>
<td>4.1 and up</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Downloads</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>306,014,906</td>
<td>02.08.18</td>
</tr>
</tbody>
</table>
tapas.net

- model=GT-I9300 & vendor=Samsung
- op=2501
- pkg=com.some.app
- ll=47.6144939,-122.1964071
- Mitigation: limit permissions
<table>
<thead>
<tr>
<th>Updated</th>
<th>Size</th>
<th>Installs</th>
<th>Current Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 7, 2018</td>
<td>Varies with device</td>
<td>100,000,000 - 500,000,000</td>
<td></td>
</tr>
<tr>
<td>February 8, 2018</td>
<td>Varies with device</td>
<td>100,000,000 - 500,000,000</td>
<td>2.1.5.2</td>
</tr>
<tr>
<td>February 7, 2018</td>
<td></td>
<td></td>
<td>4.1.7.1.14</td>
</tr>
<tr>
<td>Updated</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>February 7, 2018</td>
<td></td>
<td>10,000,000 - 50,000,000</td>
<td></td>
</tr>
<tr>
<td>Updated</td>
<td></td>
<td>10,000,000 - 50,000,000</td>
<td>1.6.4</td>
</tr>
<tr>
<td>Updated</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>February 7, 2018</td>
<td></td>
<td>10,000,000 - 50,000,000</td>
<td>1.5.3</td>
</tr>
<tr>
<td>Updated</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
&dpi=160&screenresolution=320x480
&androidversion=16&istablet=false
&manufacturer=samsung&devicename=m0
&connectiontype=EDGE&operator=MTC
&aid=83acb4abaf9ac91e
&tlat=0.0&tlon=0.0
<table>
<thead>
<tr>
<th>Updated</th>
<th>Installs</th>
<th>Current Version</th>
<th>Requires Android</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 3, 2018</td>
<td>10,000 - 50,000</td>
<td>1.0</td>
<td>4.0 and up</td>
</tr>
<tr>
<td>December 14, 2017</td>
<td>10,000 - 50,000</td>
<td>3.1.6zg</td>
<td></td>
</tr>
<tr>
<td>February 6, 2018</td>
<td>100,000 - 500,000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
GET
GET

POST
cmd_type_install_app

[device info], [android id], [imei], [imsi]
<table>
<thead>
<tr>
<th>Updated</th>
<th>Installs</th>
<th>Current Version</th>
<th>Updated</th>
<th>Installs</th>
<th>Current Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 7, 2018</td>
<td>10,000,000 - 50,000,000</td>
<td>1.6.8_ww</td>
<td>February 7, 2018</td>
<td>10,000,000 - 50,000,000</td>
<td>1.5.46_ww</td>
</tr>
<tr>
<td>February 7, 2018</td>
<td>500,000,000 - 1,000,000,000</td>
<td>4.0.28_ww</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>November 3, 2017</td>
<td>10,000,000 - 50,000,000</td>
<td>2.0.18_ww</td>
<td>January 25, 2018</td>
<td>10,000,000 - 50,000,000</td>
<td>2.0.48_ww</td>
</tr>
</tbody>
</table>
- Device information
- Network information
- GPS coordinates
- Mitigation: limit permissions

- Camera
- NFC
- Bluetooth
- Microphone
- Location
UserData v1 = MMSDK.getUserData();
if(v1 != null) {
    v0 = new JSONObject();
    v0.put("age", v1.getAge());
    v0.put("kids", v1.getChildren());
    v0.put("hhi", v1.getIncome());
    v0.put("edu", v1.getEducation());
    v0.put("eth", v1.getEthnicity());
    v0.put("gender", v1.getGender());
    v0.put("keywords", JSONUtils.buildFromList(UUtils.s
    v0.put("marital", v1.getMarital());
    v0.put("politics", v1.getPolitics());
    v0.put("zip", v1.getPostalCode());
    Date v2 = v1.getDob();
    if(v2 != null) {
        v0.put("dob", new SimpleDateFormat("yyyyMMdd")
    }
    v0.put("state", v1.getState());
    v0.put("country", v1.getCountry());
    v0.put("dma", v1.getDma());
<table>
<thead>
<tr>
<th>Updated</th>
<th>Installs</th>
<th>Requires Android</th>
<th>Updated</th>
<th>Installs</th>
<th>Requires Android</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 31, 2018</td>
<td>500,000,000 - 1,000,000,000</td>
<td>4.1 and up</td>
<td>February 12, 2018</td>
<td>100,000,000 - 500,000,000</td>
<td>4.0.3 and up</td>
</tr>
<tr>
<td>February 11, 2018</td>
<td>Varies with device</td>
<td></td>
<td>January 31, 2018</td>
<td>100,000,000 - 500,000,000</td>
<td>4.1 and up</td>
</tr>
<tr>
<td>February 5, 2018</td>
<td>Varies with device</td>
<td></td>
<td>February 8, 2018</td>
<td>100,000,000 - 500,000,000</td>
<td>4.1 and up</td>
</tr>
<tr>
<td>February 11, 2018</td>
<td>Varies with device</td>
<td></td>
<td>February 12, 2018</td>
<td>100,000,000 - 500,000,000</td>
<td>4.1 and up</td>
</tr>
</tbody>
</table>
• Device information
• GPS coordinates
• Personal information (DOB, name, gender, email, etc)
• App usage
• Mitigation: update SDK’s
<table>
<thead>
<tr>
<th>Updated</th>
<th>Installs</th>
<th>Current Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 29, 2017</td>
<td>10,000,000 - 50,000,000</td>
<td>4.0.20171228.1</td>
</tr>
<tr>
<td>January 31, 2018</td>
<td>10,000,000 - 50,000,000</td>
<td>3.4.5</td>
</tr>
<tr>
<td>January 29, 2018</td>
<td>5,000,000 - 10,000,000</td>
<td>2.2.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Updated</th>
<th>Installs</th>
<th>Requires Android</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 29, 2018</td>
<td>1,000,000 - 5,000,000</td>
<td>4.0.3 and up</td>
</tr>
<tr>
<td>January 17, 2018</td>
<td>1,000,000 - 5,000,000</td>
<td>3.6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Updated</th>
<th>Size</th>
<th>Installs</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 31, 2018</td>
<td>Varies with device</td>
<td>1,000,000 - 5,000,000</td>
</tr>
<tr>
<td>January 25, 2018</td>
<td>Varies with device</td>
<td>1,000,000 - 5,000,000</td>
</tr>
</tbody>
</table>
[Full request URI: http://api.allconnected.in/abc/activate/]

[HTTP request 1/2]
[Response in frame: 63]
[Next request in frame: 65]

File Data: 394 bytes

JavaScript Object Notation: application/json

Object
  ▷ Member Key: dev_model
  ▷ Member Key: phone_number
  ▷ Member Key: os_lang
  ▷ Member Key: os_ver
  ▷ Member Key: google_account
  ▷ Member Key: imei
  ▷ Member Key: app_ver_code
  ▷ Member Key: dev_mac_addr
  ▷ Member Key: app_uuid
  ▷ Member Key: network_name
  ▷ Member Key: app_dist_channel
  ▷ Member Key: dev_manufacturer
  ▷ Member Key: network_code
  ▷ Member Key: os_name
  ▷ Member Key: app_package_name

```
put(v5, getLine1Number);
put("google_account", VpnUtils.getGoogleAccount(arg8));
put("os_name", "Android");
put("os_ver", Build$VERSION.RELEASE);
put("os_lang", Locale.getDefault().toString());
put("dev_id", Settings$Secure.getString(arg8.getConten
```
[Full request URI: http://boxoofeast-webservice.azurewebsites.net/ECService.svc/json/getListeLieux]

[HTTP request 1/1]

[Response in frame: 174]

File Data: 139 bytes

JavaScript Object Notation: application/json

Object

- Member Key: filtre
  - Object
    - Member Key: idVilleRecherche
    - Member Key: soiree
    - Member Key: idCategorie
    - Member Key: rechercheVille
    - Member Key: distKm
    - Member Key: longitude
    - Member Key: kids
    - Member Key: latitude
&asver=16&aver=4.1.2
&brand=samsung&ch=xiaomi&co=US
&imei=369214967775679
&lang=en&model=GT-I9300&net=gprs
&packageName=com.some.app
&ph=+5047394794295
&ppi=320x480
LEAKED DATA

- IMEI, IMSI, android_id
- Device information
- Location
- Personal information
- Phone number
- Email address
Why is it wrong?

- Data can be intercepted
- Data can be modified
- Bypassing Android permission system
User

- Control app permissions
- Use VPN
- Check apps
• Do not use HTTP
• Encrypt all data

```java
private byte[] encryptPart(byte[] arg5) throws InvalidKeyException {
    Cipher v0 = Cipher.getInstance("RSA/None/PKCS1Padding");
    v0.init(1, this.publicKey);
    return v0.doFinal(arg5);
}
```
Developer

- Do not use HTTP
- Encrypt all data
- Update 3rd party SDKs
- Test app for HTTP requests before publishing
isCleartextTrafficPermitted

- >= Android 6
- >= Android 8 in WebView
- >= Android 9 - **False** by default
HTTP vs HTTPS in Apps
FINDINGS

- 90% of APPs are still using HTTP
- Exposing device information, user information, GPS coordinates
- Due to 3rd party SDK’s
THANK YOU!
QUESTIONS?

Roman Unuchek
Security Researcher
Kaspersky Lab