RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: ASEC-T08

LEAKING ADS – IS USER DATA TRULY SECURE?

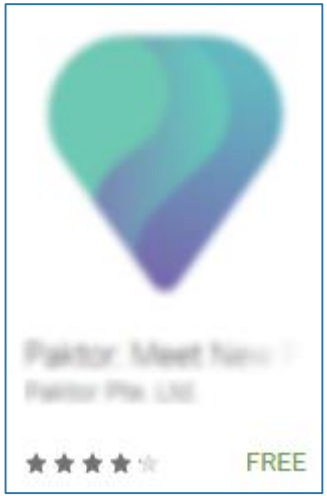
Roman Unuchek

Security Researcher
Kaspersky Lab

FINDINGS

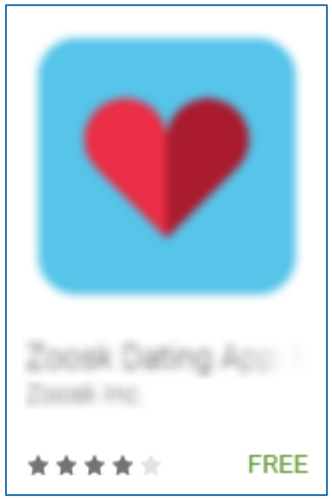
- 4 million apks exposing data
- Device information, user information, GPS coordinates
- Advertising SDK's

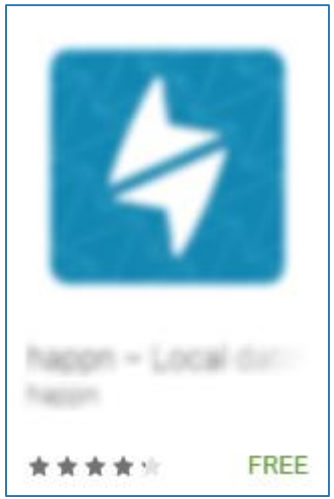
THE BEGINNING



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

THE BEGINNING

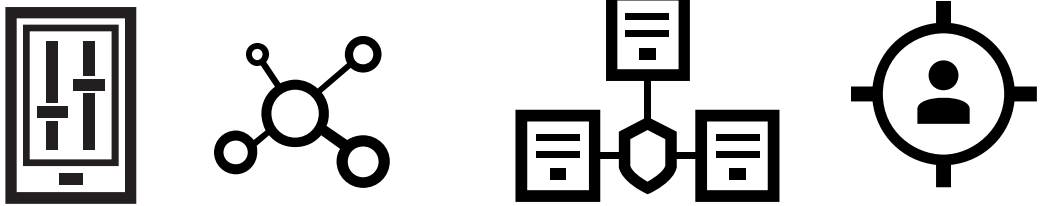




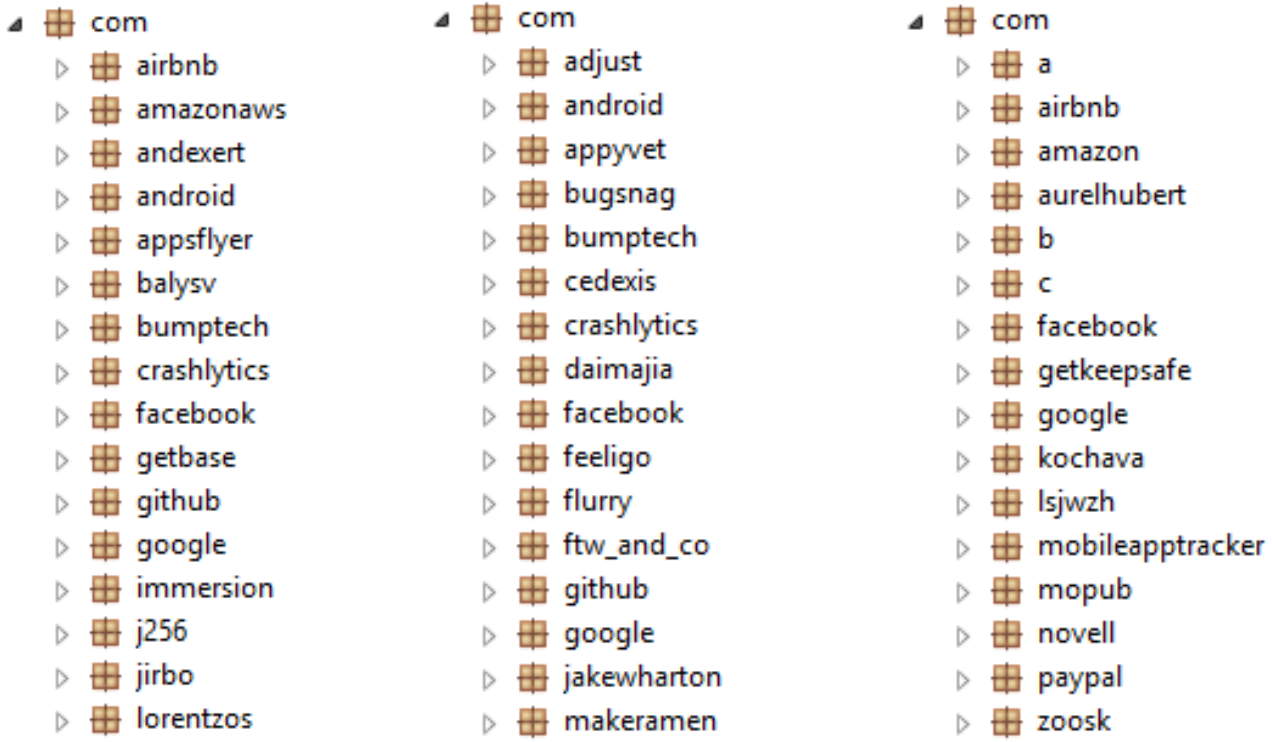
- Device information
- Personal information (age, gender)
- GPS coordinates

My own Device

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

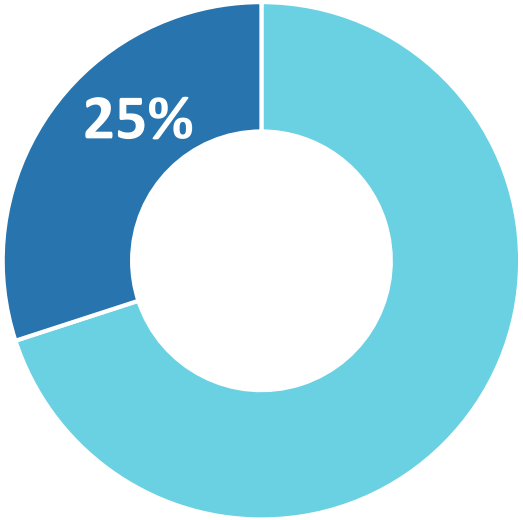


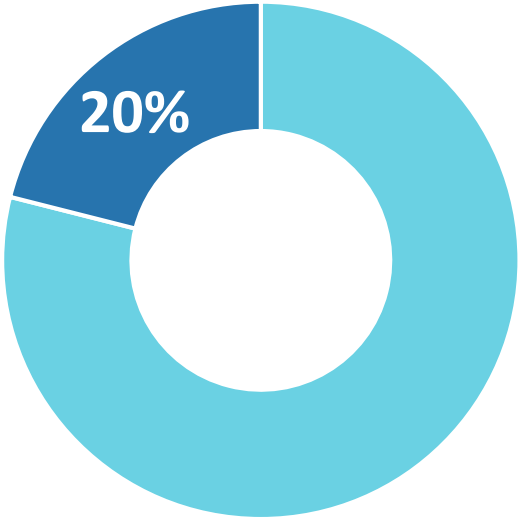
SDKs

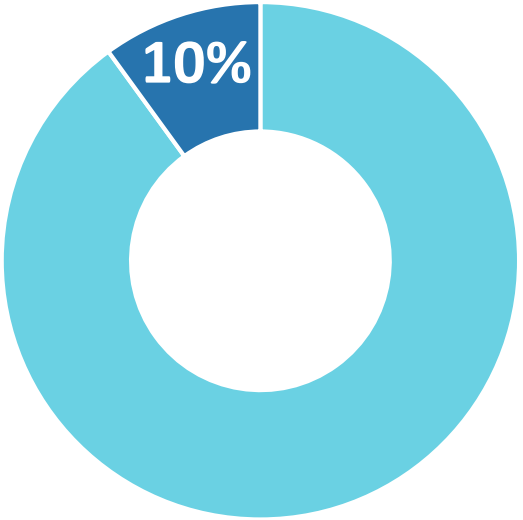

com
airbnb
amazonaws
andexert
android
appsflyer
balysv
bumptech
crashlytics
facebook
getbase
github
google
immersion
j256
jirbo
lorentzos
com
adjust
android
appyvet
bugsnag
bumptech
cedexis
crashlytics
daimajia
facebook
feeligo
flurry
ftw_and_co
github
google
jakewharton
makeramen
com
a
airbnb
amazon
aurelhubert
b
c
facebook
getkeepsafe
google
kochava
lsjwzh
mobileapptracker
mopub
novell
paypal
zoosk

SDKs

3rd party code in APPs







DATA

- Since 2014, more than 4 years!
- 13,622,391 APK files
- 131,203,322 unique urls
- 14,906,467 PCAP files

DATA

GET

POST

TOP URLs

mopub.com	apps.ad-x.co.uk
rayjump.com	typany.com
9apps.com	mobpowertech.com
advertise.1mobile.com	api.zephyr-digital.com
applovin.com	salmonads.com
tapas.net	lds.lenovomm.com
appsgeyser.com	afric.wocao.in
appioapp.com	config.cloudzad.com
taobao.com	m.mobogenie.com
duapps.com	cabinet.taximaxim.ru

mopub.com

- &dn=samsung,GT-I9300,m0xx [device info]
- &w=320&h=480 [device info]
- &mcc=624&mnc=1 [network info]
- &bundle=com.some.app [app name]
- &q=gender:m,age:27 [personal info]
- &ll=47.6144939,-122.1964071 [coordinates]
- Mitigation: do not provide user data to 3rd parties

mopub.com

Updated January 30, 2018	**Size** Varies with device	**Installs** 100,000,000 - 500,000,000	Editors' Choice 4.4 5,973,240	**Installs** 50,000,000 - 100,000,000
Updated January 10, 2018	**Size** Varies with device	**Installs** 100,000,000 - 500,000,000	Editors' Choice	**Installs** 10,000,000 - 50,000,000
Updated December 15, 2017	**Size** Varies with device	**Installs** 100,000,000 - 500,000,000	4.4 7,047,047	**Installs** 5,000,000 - 10,000,000
Updated January 10, 2018	**Installs** 100,000,000 - 500,000,000	**Requires Android** 4.1 and up		**Installs** 1,000,000 - 5,000,000
Updated January 28, 2018	**Installs** 100,000,000 - 500,000,000	**Requires Android** 4.0 and up		**Installs** 500,000 - 1,000,000
				Installs 100,000 - 500,000

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

rayjump.com

Updated February 7, 2018	**Installs** 500,000,000 - 1,000,000,000	**Current Version** 4.0.28_ww
Updated February 6, 2018	**Size** Varies with device	**Installs** 500,000,000 - 1,000,000,000
Permissions 21	Downloads 306,014,906	Date 02.08.18
Updated January 28, 2018	**Installs** 100,000,000 -	**Requires Android** 4.0 and up
Updated January 31, 2018	**Size** Varies with device	**Installs** 100,000,000 - 500,000,000

Updated February 7, 2018	**Installs** 100,000,000 - 500,000,000	**Requires Android** 4.0.3 and up
Updated February 8, 2018	**Size** Varies with device	**Installs** 100,000,000 - 500,000,000
Updated January 23, 2018	**Size** Varies with device	**Installs** 100,000,000 - 500,000,000
Updated February 8, 2018	**Installs** 100,000,000 - 500,000,000	**Requires Android** 4.1 and up

tapas.net

- &model=GT-I9300&vendor=Samsung [device info]
- &op=2501 [network info]
- &pkg=com.some.app [app name]
- &ll=47.6144939,-122.1964071 [coordinates]
- Mitigation: limit permissions

tapas.net

Updated	Size	Installs
February 7, 2018	Varies with device	100,000,000 - 500,000,000

Updated	Size	Installs
February 8, 2018	Varies with device	100,000,000 - 500,000,000

Updated	Installs	Current Version
February 7, 2018	50,000,000 - 100,000,000	2.1.5.2

Updated	Installs	Current Version
February 8, 2018	100,000,000 - 500,000,000	4.1.7.1.14

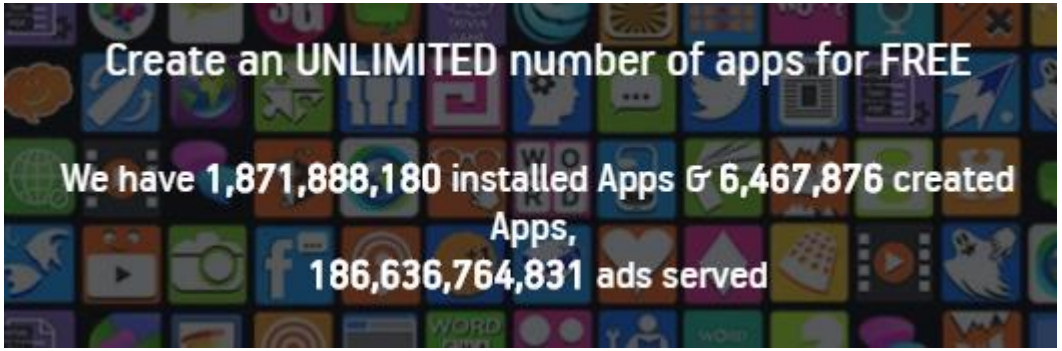
Updated	Installs	Current Version
February 1, 2018	10,000,000 - 50,000,000	1.6.4
February 8, 2018	10,000,000 - 50,000,000	1.5.3

Updated	Size	Installs
February 7, 2018	Varies with device	10,000,000 - 50,000,000

appsgeyser.com

- &dpi=160&screenresolution=320x480 [device info]
- &androidversion=16&istablet=false [device info]
- &manufacturer=samsung&devicename=m0 [device info]
- &connectiontype=EDGE&operator=MTC [network info]
- &aid=83acb4abaf9ac91e [android id]
- &tlat=0.0&tlon=0.0 [coordinates]

appsgeyser.com



Updated	**Installs**	**Current Version**
February 3, 2018	10,000 - 50,000	1.0
Updated	**Installs**	**Current Version**
December 14, 2017	10,000 - 50,000	3.1.6zg
Updated	**Installs**	**Requires Android**
February 6, 2018	100,000 - 500,000	4.0 and up

GET

GET

GET

POST

ushareit.com

[Full request URI: http://cm.ushareit.com/relayserver/1.0/cmds]
[HTTP request 1/1]
[Response in fra
File Data: 677 by
JavaScript Object No
Object
Member Key: exist_cmd_ids
String value: []
Key: exist_cmd_ids
Member Key: params
String value [truncated]: {"device_category hone","os_ver":16,"screen_width":320,"device_id":"a.83acb4abaf9ac91e",
Key: params
Member Key: support_cmd_types
String value: ["cmd_type_personal","cmd_type_install_app","cmd_type_notification","cmd_type_remove","cmd_type_feed","
Key: support_cmd_types

cmd_type_install_app

[device info], [android id], [imei], [imsi]

ushareit.com

Updated	Installs	Current Version
February 7, 2018	10,000,000 - 50,000,000	1.6.8_ww

Updated	Installs	Current Version
February 7, 2018	10,000,000 - 50,000,000	1.5.46_ww

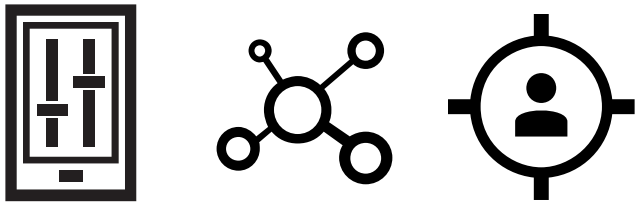
Updated	Installs	Current Version
February 7, 2018	500,000,000 - 1,000,000,000	4.0.28_ww

Updated	Installs	Current Version
November 3, 2017	10,000,000 - 50,000,000	2.0.18_ww

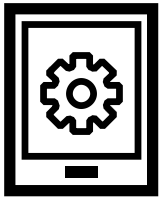
Updated	Installs	Current Version
January 25, 2018	10,000,000 - 50,000,000	2.0.48_ww

nexage.com

- Device information
- Network information
- GPS coordinates
- Mitigation: limit permissions



- Camera
- NFC
- Bluetooth
- Microphone
- Location



nexage.com

```
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(Utils.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());
```

[Kids]
[Income]
[Education]
[Ethnicity]

[Politics]

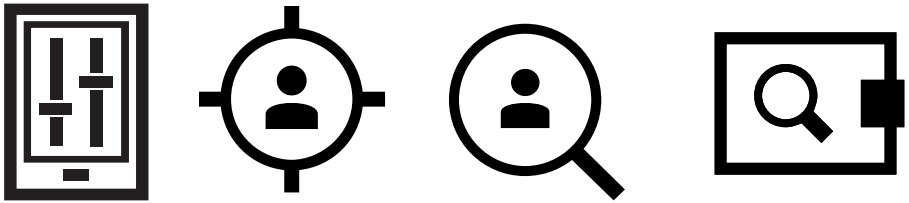
nexage.com

Updated	Installs	Requires Android
January 31, 2018	500,000,000 - 1,000,000,000	4.1 and up
February 12, 2018	100,000,000 - 500,000,000	4.0.3 and up
January 31, 2018	100,000,000 - 500,000,000	4.1 and up
February 8, 2018	100,000,000 - 500,000,000	4.1 and up
February 12, 2018	100,000,000 - 500,000,000	4.1 and up

Updated	Size	Installs
February 11, 2018	Varies with device	100,000,000 - 500,000,000
February 5, 2018	Varies with device	100,000,000 - 500,000,000
February 11, 2018	Varies with device	100,000,000 - 500,000,000

quantumgraph.com

- Device information
- GPS coordinates
- Personal information (DOB, name, gender, email, etc)
- App usage
- Mitigation: update SDK's



quantumgraph.com

Updated	Installs	Current Version
December 29, 2017	10,000,000 - 50,000,000	4.0.20171228.1
January 31, 2018	10,000,000 - 50,000,000	3.4.5
January 29, 2018	5,000,000 - 10,000,000	2.2.0

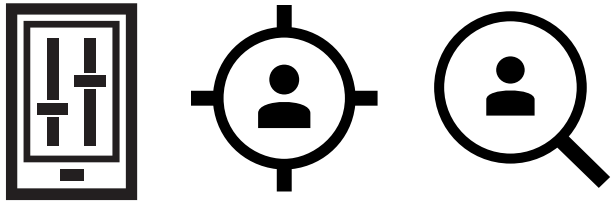
Updated	Installs	Requires Android
January 29, 2018	1,000,000 - 5,000,000	4.0.3 and up
January 17, 2018	1,000,000 - 5,000,000	3.6

Updated	Size	Installs
January 31, 2018	Varies with device	1,000,000 - 5,000,000
January 25, 2018	Varies with device	1,000,000 - 5,000,000

other


```
[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.getContent
```



CLOUDS

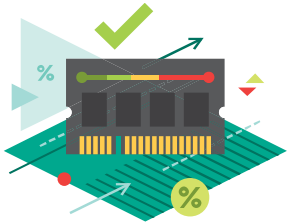

```
[Full request URI: http://boxofeast-webservice.azurewebsites.net/ECService.svc/json/getListeLieux]
[HTTP request 1/1]
[Response in frame: 174]
File Data: 139 bytes
JavaScript Object Notation: application/json
  Object
    Member Key: filtre
      Object
        Member Key: idVilleRecherche
        Member Key: soiree
        Member Key: idCategorie
        Member Key: rechercheVille
        Member Key: distKm
        Member Key: longitude
        Member Key: kids
        Member Key: latitude
```

CLOUDS

http://ir-2016137559.cn-north-1.elb.amazonaws.com.cn/api/v3/up.php?appid=106a4e0b2f
&asver=16&aver=4.1.2
&brand=samsung&ch=xiaomi&co=US
&imei=**369214967775679** [imei]
&lang=en&model=GT-I9300&net=gprs
&packageName=com.some.app
&ph=**+5047394794295** [phone number]
&ppi=320x480

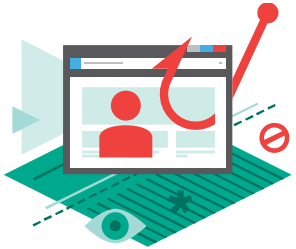
LEAKED DATA

- IMEI, IMSI, android_id
- Device information
- Location
- Personal information
- Phone number
- Email address



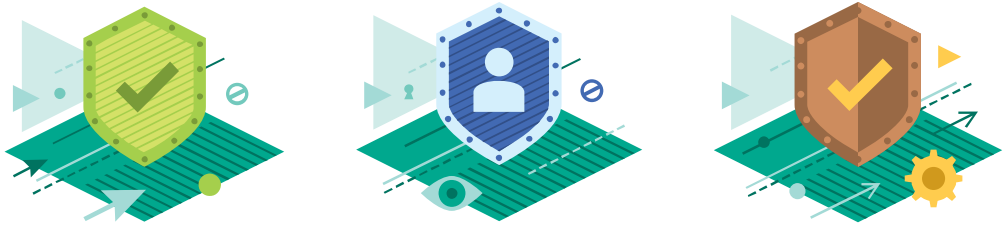
Why is it wrong?

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



User

- Control app permissions
- Use VPN
- Check apps



Developer

- Do not use HTTP
- Encrypt all data

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

[RSA]

Developer

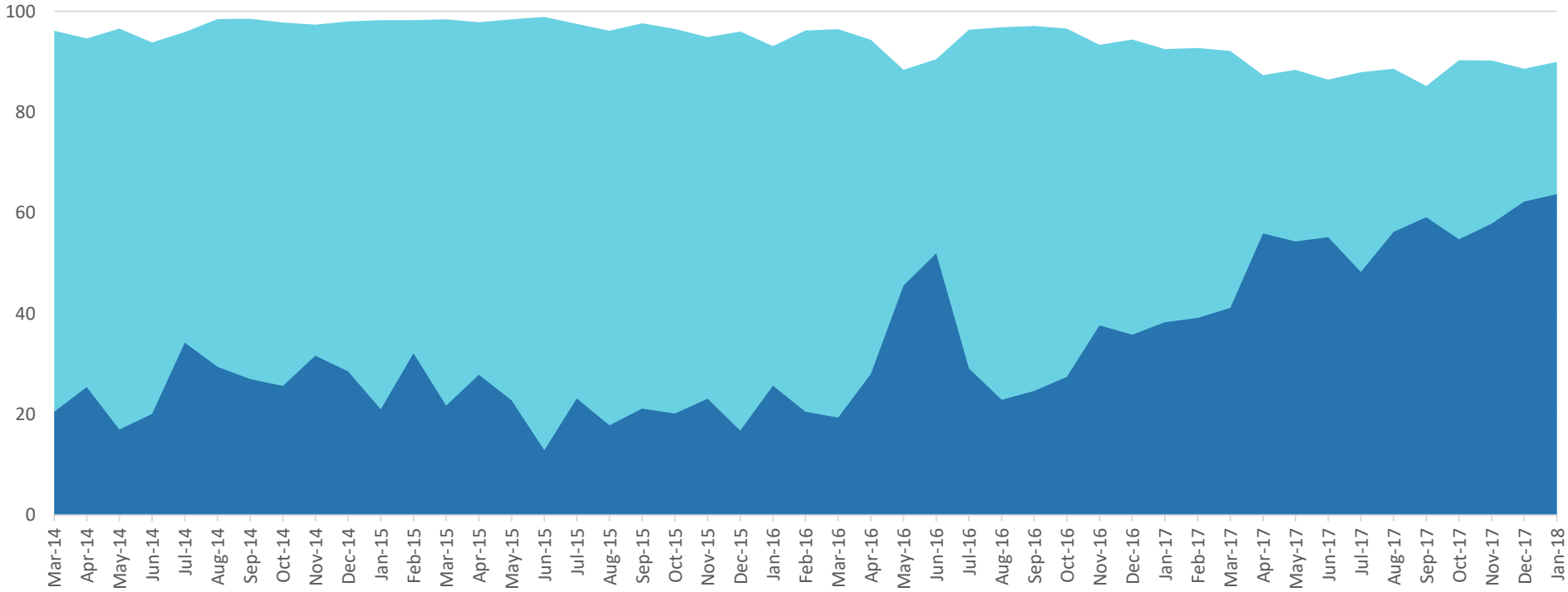
- Do not use HTTP
- Encrypt all data
- Update 3rd party SDKs
- Test app for HTTP requests before publishing

Developer

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

RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: ASEC-T08

THANK YOU!
QUESTIONS?

Roman Unuchek

Security Researcher
Kaspersky Lab