Hacking Application mobile

Comment s’attaque une application mobile ?

Grenoble

07 mars 2024

Orange France

Introduction

Orange

Orange CyberDefense

Filiale Orange dédiée aux services aux entreprises, 3000 experts dans 20 pays

Orange France

Plus de 50 000 pers. avec un des SI parmi les plus étendus et sensibles en France

Adrien MORCHE

8 ans d'expérience en Cyber

Analyse de risque, Intégration de la sécurité dans les projets

Pentest : hacker une application (avec autorisation) & expliquer comment corriger

Lead Pentester à Orange France

Equipe réalisant ~200 pentests internes par an

Expertise personnelle pentest web, mobile (Cert. SANS SEC575), infra

Disclaimers

L'idée est de présenter un métier pas d'encourager à hacker de manière illégale

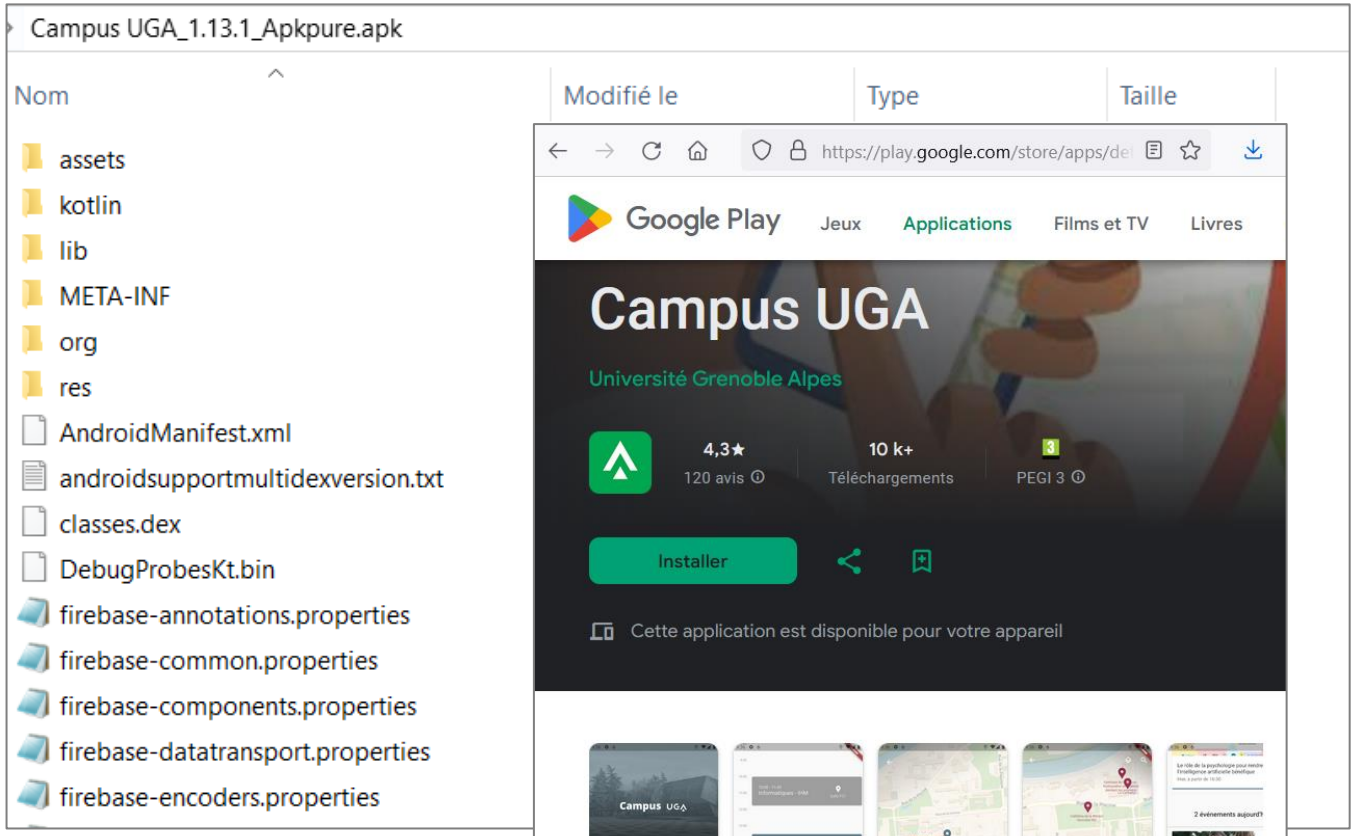
Sujet vaste : parti pris de présenter Android (mais logique proche sur IOS), hors privacy

Situation n°1 : télécharger fichier d'installation

Fichier APK (zip) accessible à tous : https://apkgk.com/APK-Downloader?package=com.uga.idexve

Similaire à une page web

- Framework : flutter
- Fonts, Images : montagnes.svg
- Config : firebase-installations.properties
- Code : js, lib (.so), classes.dex
- Backend & liens (18) :
  vie-etudiante-test.grenet.fr,
  app-campus-preprod.grenet.fr,
  app-campus.univ-grenoble-alpes.fr
  http://localhost/swagger-ui.html



Avec des spécificités :

- AndroidManifest.xml : accès localisation, accès internet, camera, nfc, vibrate, …
- Peu visuel : webview, décompileur (smali vers java)

Situation n°2 : vol de téléphone (ou spyware)

Le téléphone n'est pas un environnement inviolable

- Forte dépendance à la version Android (efforts importants pour améliorer)

Récupération des données téléphone volé

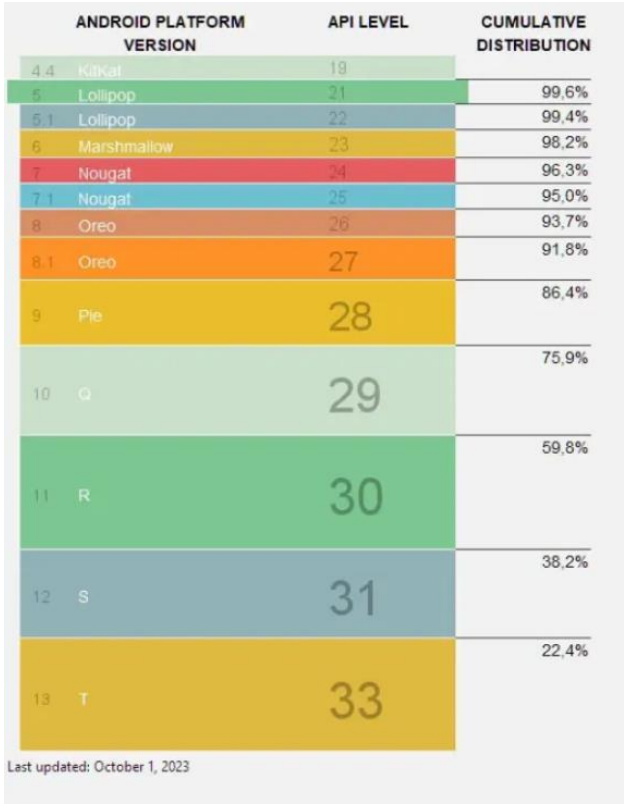
- Contourner écran verrouillage https://github.com/urbanadventurer/Android-PIN-Bruteforce

Installation application malveillante

- Accès à des ressources partagées

Les contrôles sur l'application

- Mes données sont stockées chiffrées
- Les données transitent chiffrées
- Stockage dans les logs système restreint



ANDROID PLATFORM VERSION	API LEVEL	CUMULATIVE DISTRIBUTION
4.4 KitKat	19	
5 Lollipop	21	99,6%
5.1 Lollipop	22	99,4%
6 Marshmallow	23	98,2%
7 Nougat	24	96,3%
7.1 Nougat	25	95,0%
8 Oreo	26	93,7%
8.1 Oreo	27	91,8%
9 Pie	28	86,4%
10 Q	29	75,9%
11 R	30	59,8%
12 S	31	38,2%
13 T	33	22,4%

Last updated: October 1, 2023

Le Monde

Se connecter

T PEGASUS

PROJET PEGASUS · CYBERESPIONNAGE

« Projet Pegasus » : révélations sur un système mondial d'espionnage de téléphones

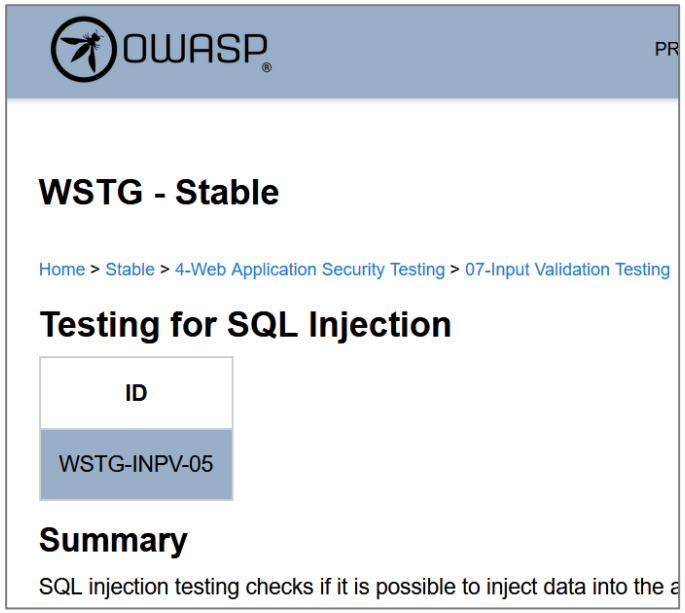
```
$ adb devices
List of devices attached
emulator-5554   device


$ adb shell
generic_x86:/ $ su
generic_x86:/ # whoami
root
generic_x86:/ # ls /data/data/com.uga*

$ adb logcat
```

Situation attaque n°3 : attaque du backend

Une fois le backend identifié (situation 1) pentest web
Et idéalement : avec un compte



Complexité intermédiaire entre client & server

- Emulation téléphone
- Ajout proxy
- Gestion du SSL

Tests identiques Web (OWASP)

- Contrôle d'accès
- Traitement entrées utilisateurs
- Sécurité souvent oubliée par les développeurs

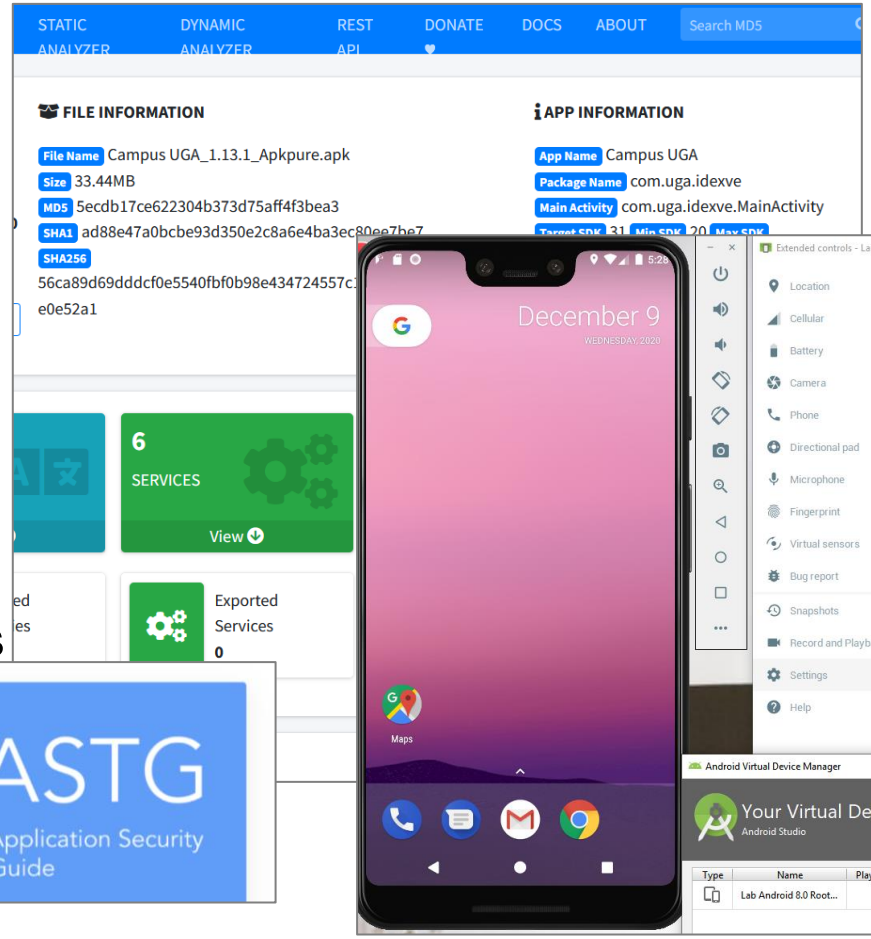
```
#editer res/xml/network_security_config.xml
<network-security-config>
    <base-config>
        <trust-anchors>
            <certificates src="sytem" />
            <certificates src="user" />
        </trust-anchors>
    </base-config>
</network-security-config>

$ apktool b app1
$ keytool -genkey -v -keystore resign.keystore -alias app1 -keyalg RSA
-validity 10000
$ jarsigner -verbose -keystore resign.keystore app1/dist/app1.apk app1
(optionel)# zipalign -fv 4 app1.apk app1/dist/app1.apk
$ adb uninstall com.app1
$ adb install app1/dist/app1.apk
```

Outils : pour les curieux

Dans une démarche de recherche légale sur des applications autorisées

- **MobSF** : analyse statique
- Bycodeviewer : plusieurs décompileurs
- Android Studio : émuler un téléphone (rooté) (>Tools>AVD Manager)
- Burp Suite : pour l'analyse du backend
- Frida (et objection) : pour désactiver certaines sécurités et « patcher » l'application à la volée



Pour les précautionneux :

- Mettez votre téléphone à jour (dès le choix du modèle)
- Utilisez des stores de confiance
- Utilisez un déverrouillage écran robuste
- Considérez votre téléphone comme faillible

```
$ objection -g com.orange.app explore
[usb]# android sslpinning disable
(agent) Custom TrustManager ready, overriding SSLContext.init()
(agent) Found  com.orange.app.security.TrustManangerImpl,
overriding TrustManangerImpl.verifyChain()
(agent) Registering job azgzegazd. Type: android-sslpinning-
disable
[usb]# android root disable
(agent) Registering job azgzegazd. Type: root-detection-disable
```

Merci

Soyez curieux mais surtout…
soyez responsables