Ardui-no pown Android

A. Cervoise
antoine.cervoise@gmail.com

NTT Communications
NTT Com Security

July 6, 2016

Summary

Powning Android

Arduino

Enable mode debug

Install APK

Conclusion

Attacks against Android

Interesting here

- Attack through debug mode
- Installing APK

Not interesting here

- Access through ClockworkMod
- Reading the RAM

Debug Mode Attack

```
Root the phone

adb pull /data/system/gesture.key ./gesture.key
adb pull /data/system/password.key ./password.key

adb pull /data/data/com.android.providers.settings/
 databases/settings.db ./settings.db
adb pull /dbdata/databases/com.android.providers.settings
 /settings.db    ./settings.db

Extract gesture hash (not salt) or password/pin
 hash and salt
```

Then *john*

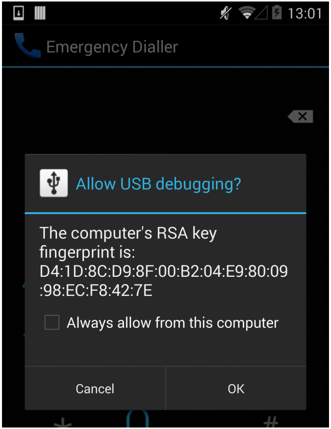
About Android Debug Mode

Debug mode enable

- Before Android 4.2.2 : Allow debug mode
- Android 4.2.2-4.4.2 : Debug mode need validation (Secure USB), can be bypassed
- Since Android 4.4.3 : Secure USB debug mode

About Android Debug Mode

USB confirmation dialog on the emergency dialer (when phone is locked)



Allow USB debugging?

The computer's RSA key fingerprint is: D4:1D:8C:D9:8F:00:B2:04:E9:80:09 :98:EC:F8:42:7E

□ Always allow from this computer

https://labs.mwrinfosecurity.com/advisories/android-4-4-2-secure-usb-debugging-bypass/

About Android Debug Mode

Samsung B7510 enable debug mode each time USB is plugged

About installing apk

- On Play Store: is ”audited” by Google
- Directly with the APK: need to allow unknown sources

Summary

Powning Android

Arduino

Enable mode debug

Install APK

Conclusion

Arduino

Emulate keyboard

- https://github.com/samratashok/Kautilya
- https://github.com/offensive-security/hid-backdoor-peensy

Summary

Powning Android

Arduino

Enable mode debug

Install APK

Conclusion

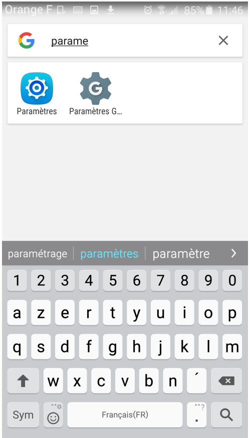
Open settings

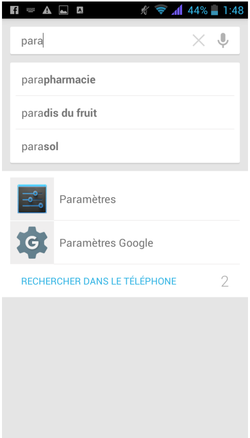
Samsung Galaxy S6
Android 5.1.1

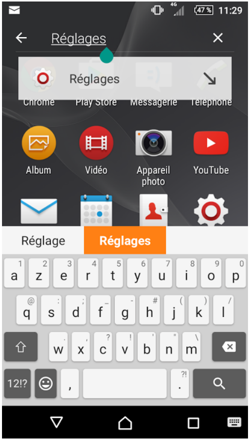
Polaroid
PROS08BPR001
Unknown Android

Sony Xperia Z1
Compact
Android 5.1.1

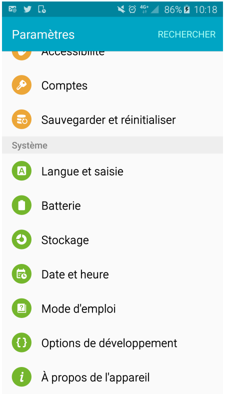
Open settings

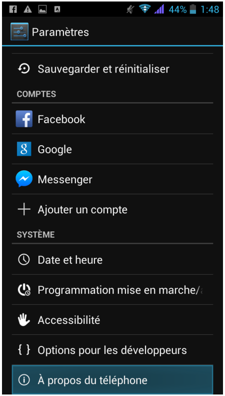


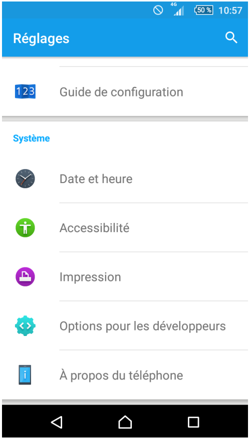




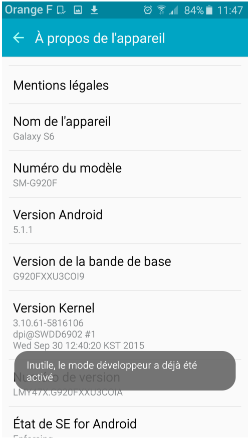
About phone


86% 10:18
Paramètres
RECHERCHER
Accessibilité
Comptes
Sauvegarder et réinitialiser
Système
Langue et saisie
Batterie
Stockage
Date et heure
Mode d'emploi
Options de développement
À propos de l'appareil


44% 1:48
Paramètres
Sauvegarder et réinitialiser
COMPTES
Facebook
Google
Messenger
Ajouter un compte
SYSTÈME
Date et heure
Programmation mise en marche/
Accessibilité
{ } Options pour les développeurs
À propos du téléphone


50 % 10:57
Réglages
123
Guide de configuration
Système
Date et heure
Accessibilité
Impression
Options pour les développeurs
À propos du téléphone

Activate developper mode



À propos de l'appareil

Mentions légales

Nom de l'appareil
Galaxy S6

Numéro du modèle
SM-G920F

Version Android
5.1.1

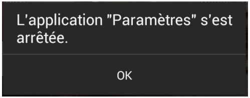
Version de la bande de base
G920FXXU3COI9

Version Kernel
3.10.61-5816106
dpi@SWDD6902 #1
Wed Sep 30 12:40:20 KST 2015

Inutile, le mode développeur a déjà été activé

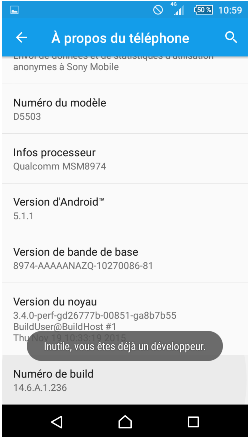
Numéro de version
LMY47X.G920FXXU3COIA

État de SE for Android



L'application "Paramètres" s'est arrêtée.

OK



À propos du téléphone

Envoi de données et de statistiques d'utilisation anonymes à Sony Mobile

Numéro du modèle
D5503

Infos processeur
Qualcomm MSM8974

Version d'Android™
5.1.1

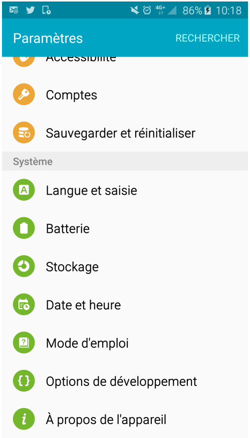
Version de bande de base
8974-AAAAANAZQ-10270086-81

Version du noyau
3.4.0-perf-gd26777b-00851-ga8b7b55
BuildUser@BuildHost #1
Thu Nov 19 10:33:19 2015

Inutile, vous êtes déjà un développeur.

Numéro de build
14.6.A.1.236

Developper mode


86% 10:18

Paramètres RECHERCHER

Accessibilité

Comptes

Sauvegarder et réinitialiser

Système

Langue et saisie

Batterie

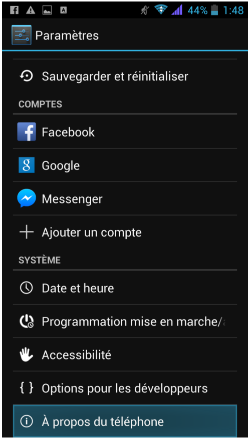
Stockage

Date et heure

Mode d'emploi

Options de développement

À propos de l'appareil


44% 1:48

Paramètres

Sauvegarder et réinitialiser

COMPTES

Facebook

Google

Messenger

Ajouter un compte

SYSTÈME

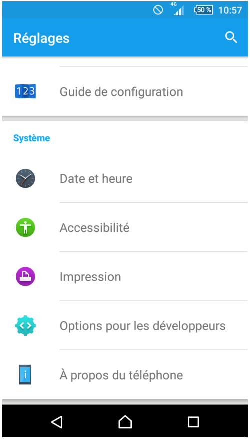
Date et heure

Programmation mise en marche/

Accessibilité

Options pour les développeurs

À propos du téléphone


50 % 10:57

Réglages

Guide de configuration

Système

Date et heure

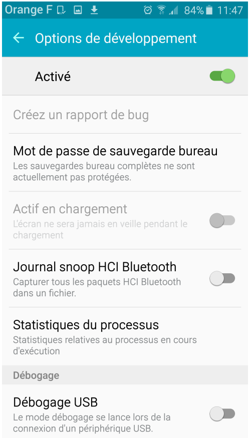
Accessibilité

Impression

Options pour les développeurs

À propos du téléphone

Activate debug mode



Options de développement

Activé

Créez un rapport de bug

Mot de passe de sauvegarde bureau
Les sauvegardes bureau complètes ne sont actuellement pas protégées.

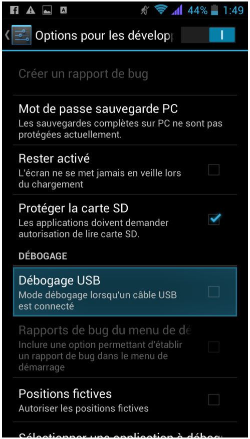
Actif en chargement
L'écran ne sera jamais en veille pendant le chargement

Journal snoop HCI Bluetooth
Capturer tous les paquets HCI Bluetooth dans un fichier.

Statistiques du processus
Statistiques relatives au processus en cours d'exécution

Débogage

Débogage USB
Le mode débogage se lance lors de la connexion d'un périphérique USB.



Options pour les dévelop

Créer un rapport de bug

Mot de passe sauvegarde PC
Les sauvegardes complètes sur PC ne sont pas protégées actuellement.

Rester activé ☐
L'écran ne se met jamais en veille lors du chargement

Protéger la carte SD ☑
Les applications doivent demander autorisation de lire carte SD.

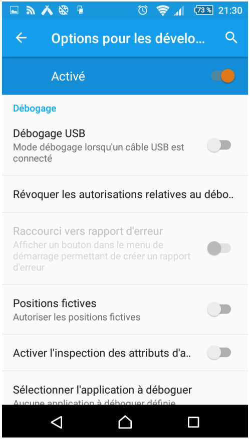
DÉBOGAGE

Débogage USB ☐
Mode débogage lorsqu'un câble USB est connecté

Rapports de bug du menu de dé ☐
Inclure une option permettant d'établir un rapport de bug dans le menu de démarrage

Positions fictives ☐
Autoriser les positions fictives

Sélectionner une application à débog



Options pour les dévelo...

Activé

Débogage

Débogage USB
Mode débogage lorsqu'un câble USB est connecté

Révoquer les autorisations relatives au débo..

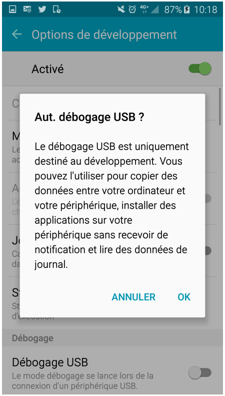
Raccourci vers rapport d'erreur
Afficher un bouton dans le menu de démarrage permettant de créer un rapport d'erreur

Positions fictives
Autoriser les positions fictives

Activer l'inspection des attributs d'a..

Sélectionner l'application à déboguer
Aucune application à déboguer définie

Debug mode warning

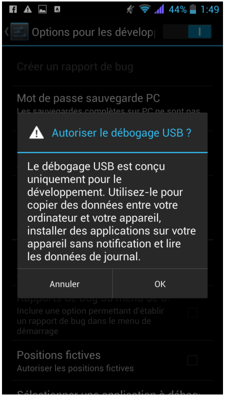


Aut. débogage USB ?

Le débogage USB est uniquement destiné au développement. Vous pouvez l'utiliser pour copier des données entre votre ordinateur et votre périphérique, installer des applications sur votre périphérique sans recevoir de notification et lire des données de journal.

Débogage USB

Le mode débogage se lance lors de la connexion d'un périphérique USB.



Mot de passe sauvegarde PC

Les sauvegardes complètes sur PC ne sont pas

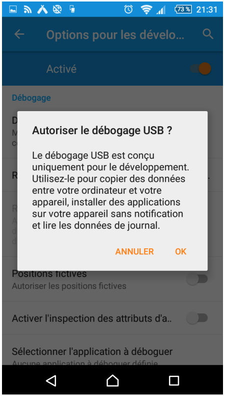
Autoriser le débogage USB ?

Le débogage USB est conçu uniquement pour le développement. Utilisez-le pour copier des données entre votre ordinateur et votre appareil, installer des applications sur votre appareil sans notification et lire les données de journal.

Inclure une option permettant d'établir un rapport de bug dans le menu de démarrage

Positions fictives

Autoriser les positions fictives



Autoriser le débogage USB ?

Le débogage USB est conçu uniquement pour le développement. Utilisez-le pour copier des données entre votre ordinateur et votre appareil, installer des applications sur votre appareil sans notification et lire les données de journal.

Positions fictives

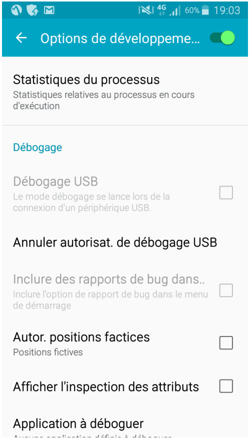
Autoriser les positions fictives

Activer l'inspection des attributs d'a..

Sélectionner l'application à déboguer

Aucune application à déboguer définie

MDM



4G 60% 19:03

Options de développeme...

Statistiques du processus
Statistiques relatives au processus en cours d'exécution

Débogage

Débogage USB □
Le mode débogage se lance lors de la connexion d'un périphérique USB.

Annuler autorisat. de débogage USB

Inclure des rapports de bug dans.. □
Inclure l'option de rapport de bug dans le menu de démarrage

Autor. positions factices □
Positions fictives

Afficher l'inspection des attributs □

Application à déboguer
Aucune application définie à déboguer

Summary

Powning Android

Arduino

Enable mode debug

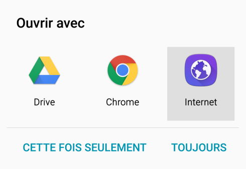
Install APK

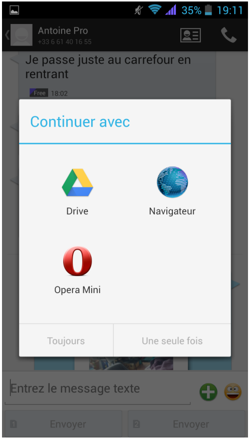
Conclusion

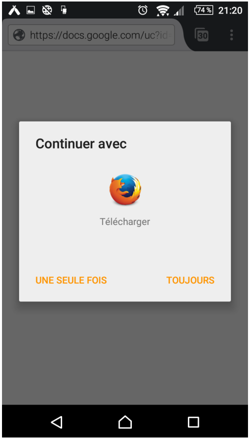
URL

`https://docs.google.com/uc?id=[...]&export=download`

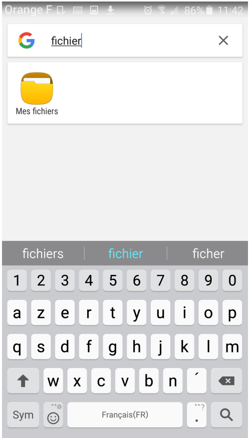
Choose browser

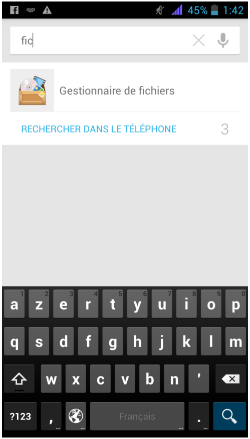


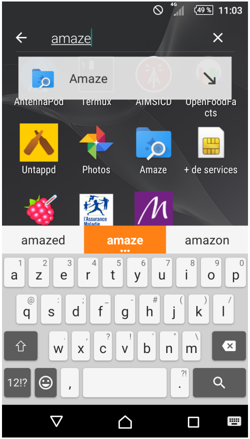

Je passe juste au carrefour en rentrant



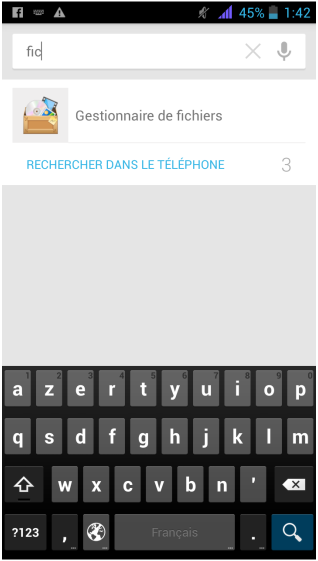
Open file application







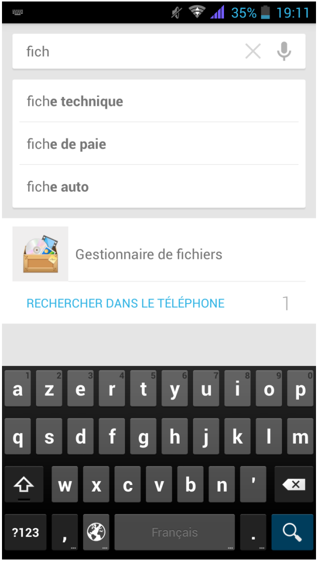
Open file application



fic

Gestionnaire de fichiers

RECHERCHER DANS LE TÉLÉPHONE 3



fich

fiche **technique**

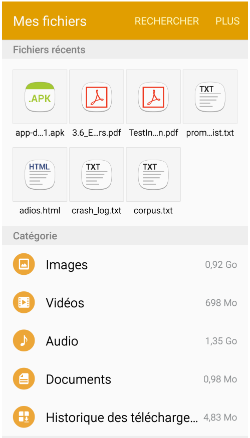
fiche **de paie**

fiche **auto**

Gestionnaire de fichiers

RECHERCHER DANS LE TÉLÉPHONE 1

File application



Mes fichiers RECHERCHER PLUS

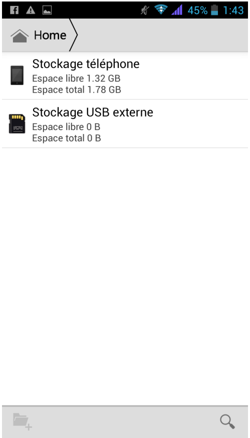
Fichiers récents

app-d...1.apk 3.6_E...rs.pdf TestIn...n.pdf prom...ist.txt

adios.html crash_log.txt corpus.txt

Catégorie

Images	0,92 Go
Vidéos	698 Mo
Audio	1,35 Go
Documents	0,98 Mo
Historique des télécharge...	4,83 Mo

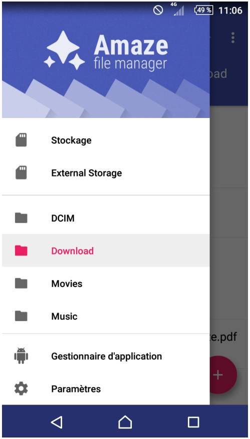


45% 1:43

Home

Stockage téléphone
Espace libre 1.32 GB
Espace total 1.78 GB

Stockage USB externe
Espace libre 0 B
Espace total 0 B

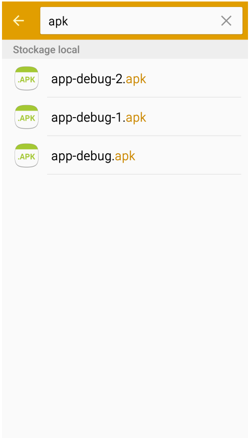


49 % 11:06

Amaze
file manager

- Stockage
- External Storage
- DCIM
- Download
- Movies
- Music
- Gestionnaire d'application
- Paramètres

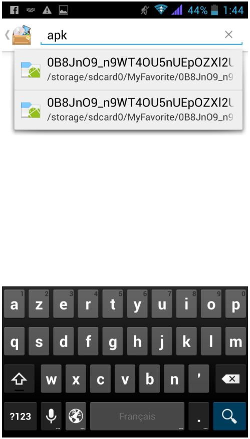
Find your apk



apk

Stockage local

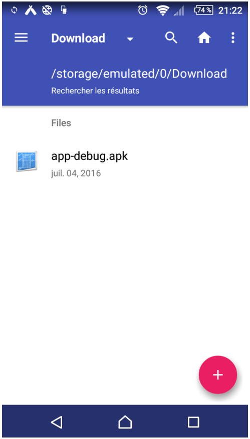
- app-debug-2.apk
- app-debug-1.apk
- app-debug.apk



apk

0B8JnO9_n9WT4OU5nUEpOZXl2U
/storage/sdcard0/MyFavorite/0B8JnO9_n9

0B8JnO9_n9WT4OU5nUEpOZXl2U
/storage/sdcard0/MyFavorite/0B8JnO9_n9



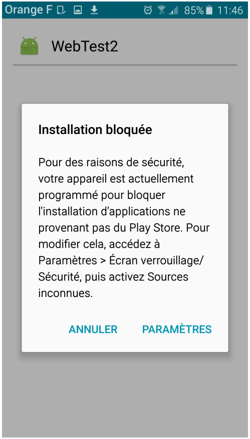
/storage/emulated/0/Download

Rechercher les résultats

Files

app-debug.apk
juil. 04, 2016

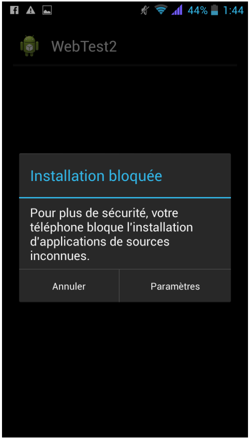
Try to install it



WebTest2

Installation bloquée

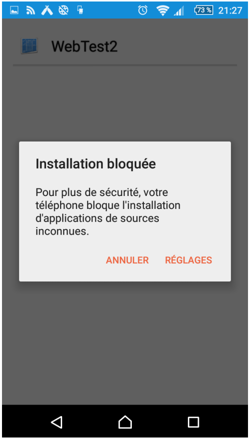
Pour des raisons de sécurité, votre appareil est actuellement programmé pour bloquer l'installation d'applications ne provenant pas du Play Store. Pour modifier cela, accédez à Paramètres > Écran verrouillage/ Sécurité, puis activez Sources inconnues.



WebTest2

Installation bloquée

Pour plus de sécurité, votre téléphone bloque l'installation d'applications de sources inconnues.

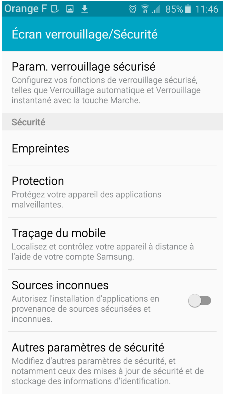


WebTest2

Installation bloquée

Pour plus de sécurité, votre téléphone bloque l'installation d'applications de sources inconnues.

Activate unknown sources



Écran verrouillage/Sécurité

Param. verrouillage sécurisé
Configurez vos fonctions de verrouillage sécurisé, telles que Verrouillage automatique et Verrouillage instantané avec la touche Marche.

Sécurité

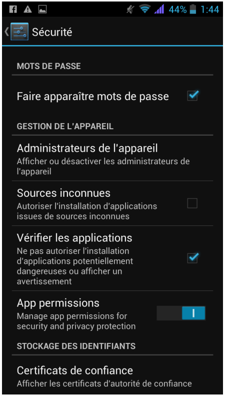
Empreintes

Protection
Protégez votre appareil des applications malveillantes.

Traçage du mobile
Localisez et contrôlez votre appareil à distance à l'aide de votre compte Samsung.

Sources inconnues □
Autorisez l'installation d'applications en provenance de sources sécurisées et inconnues.

Autres paramètres de sécurité
Modifiez d'autres paramètres de sécurité, et notamment ceux des mises à jour de sécurité et de stockage des informations d'identification.



Sécurité

MOTS DE PASSE

Faire apparaître mots de passe ☑

GESTION DE L'APPAREIL

Administrateurs de l'appareil
Afficher ou désactiver les administrateurs de l'appareil

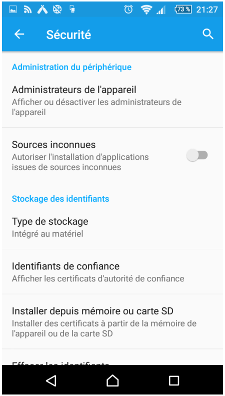
Sources inconnues □
Autoriser l'installation d'applications issues de sources inconnues

Vérifier les applications ☑
Ne pas autoriser l'installation d'applications potentiellement dangereuses ou afficher un avertissement

App permissions I
Manage app permissions for security and privacy protection

STOCKAGE DES IDENTIFIANTS

Certificats de confiance
Afficher les certificats d'autorité de confiance



Sécurité

Administration du périphérique

Administrateurs de l'appareil
Afficher ou désactiver les administrateurs de l'appareil

Sources inconnues □
Autoriser l'installation d'applications issues de sources inconnues

Stockage des identifiants

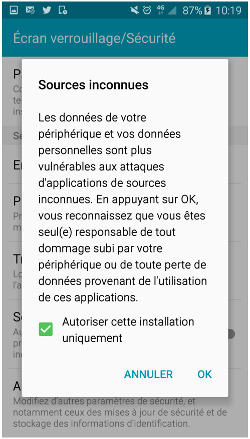
Type de stockage
Intégré au matériel

Identifiants de confiance
Afficher les certificats d'autorité de confiance

Installer depuis mémoire ou carte SD
Installer des certificats à partir de la mémoire de l'appareil ou de la carte SD

Effacer les identifiants

Last warning



87% 10:19

Écran verrouillage/Sécurité

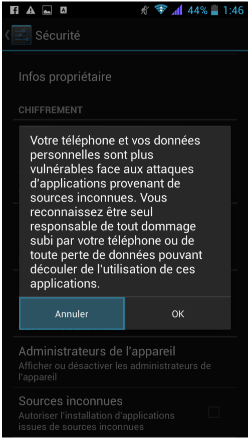
Sources inconnues

Les données de votre périphérique et vos données personnelles sont plus vulnérables aux attaques d'applications de sources inconnues. En appuyant sur OK, vous reconnaissez que vous êtes seul(e) responsable de tout dommage subi par votre périphérique ou de toute perte de données provenant de l'utilisation de ces applications.

☑ Autoriser cette installation uniquement

ANNULER OK

Modifiez d'autres paramètres de sécurité, et notamment ceux des mises à jour de sécurité et de stockage des informations d'identification.



44% 1:46

Sécurité

Infos propriétaire

CHIFFREMENT

Votre téléphone et vos données personnelles sont plus vulnérables face aux attaques d'applications provenant de sources inconnues. Vous reconnaissez être seul responsable de tout dommage subi par votre téléphone ou de toute perte de données pouvant découler de l'utilisation de ces applications.

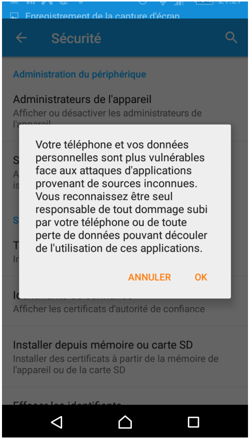
Annuler OK

Administrateurs de l'appareil

Afficher ou désactiver les administrateurs de l'appareil

Sources inconnues ☐

Autoriser l'installation d'applications issues de sources inconnues



Enregistrement de la capture d'écran

Sécurité

Administration du périphérique

Administrateurs de l'appareil

Afficher ou désactiver les administrateurs de l'appareil

Votre téléphone et vos données personnelles sont plus vulnérables face aux attaques d'applications provenant de sources inconnues. Vous reconnaissez être seul responsable de tout dommage subi par votre téléphone ou de toute perte de données pouvant découler de l'utilisation de ces applications.

ANNULER OK

Afficher les certificats d'autorité de confiance

Installer depuis mémoire ou carte SD

Installer des certificats à partir de la mémoire de l'appareil ou de la carte SD

Effacer les identifiants

Summary

Powning Android

Arduino

Enable mode debug

Install APK

Conclusion

Conlusion

Faster

- For some specific task (get the URL)
- Or if you really know the target

Conlusion

For other kind of attacks

- Fuzz Android
- Bruteforce PIN Code, password, pattern https://github.com/cervoise/Hardware-Bruteforce-Framework-2

Questions?