

# Alerte ! Ces 42 applications du Play Store cachent un logiciel malveillant

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



**Alerte ! Ces 42 applications du Play Store cachent un logiciel malveillant**

Un malware Android a une nouvelle fois été repéré sur le Google Play Store. Les chercheurs d'ESET ont en effet trouvé la trace d'un agaçant logiciel publicitaire dans le code de 42 applications en apparence inoffensive. Pour éviter d'être repéré par Google ou par leurs victimes, le malware multiplie les astuces.

Depuis un peu plus d'un an, un malware publicitaire baptisé **Android/AdDisplay.Ashas** rôde sur le Google Play Store, rapporte Lukas Stefanko, expert en sécurité informatique chez Eset. Après enquête, les chercheurs ont repéré la présence du malicieux dans 42 applications Android. Au total, ces applications ont été téléchargées par 8 millions d'internautes...[\[lire la suite\]](#)

Réagissez à cet article

## **Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :**

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

## **Quel est notre métier ?**

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques.**

## **Quel sont nos principales activités ?**

### **▪ RGPD**

- FORMATION AU RGPD
- FORMATION DE DPO
- AUDITS RGPD
- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)

### **▪ CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS
- RECHERCHE DE PREUVES

### **▪ EXPERTISES**

- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

*« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme. »*

Denis JACOPINI »

## Besoin d'un Expert ? contactez-nous

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- **Mises en conformité RGPD** ;
- Accompagnement à la mise en place de DPO ;
- **Formations** (et sensibilisations) à la **cybercriminalité** (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- **Recherche de preuves** téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- **Expertises de systèmes de vote électronique** ;



[Contactez-nous](#)



Source : *Malware Android : ces 42 applications du Play Store cachent un logiciel malveillant – PhonAndroid.com*

---

# Alerte aux possesseurs de smartphones Samsung : Effacez les empreintes enregistrées !

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



**Alerte aux possesseurs de smartphones Samsung : Effacez les empreintes enregistrées !**

Cette faille permet à un tiers de débloquer l'appareil en utilisant simplement une protection d'écran pour détourner la reconnaissance de l'empreinte.

Une faille du système de reconnaissance permet le déblocage de votre Samsung par des tiers. Le conglomérat sud-coréen a donc recommandé ce vendredi aux utilisateurs de plusieurs de ses modèles de smartphones haut de gamme d'effacer toutes les empreintes digitales enregistrées dans leur appareil...[lire la suite]

[Réagissez à cet article](#)

Quelques articles sélectionnés par notre Expert qui pourraient

## **aussi vous intéresser :**

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

## **Quel est notre métier ?**

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques.**

## **Quel sont nos principales activités ?**

### **▪ RGPD**

- FORMATION AU RGPD
- FORMATION DE DPO
- AUDITS RGPD
- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)

### **▪ CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS
- RECHERCHE DE PREUVES

### **▪ EXPERTISES**

- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES

- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

*« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.*

*Denis JACOPINI »*

## Besoin d'un Expert ? contactez-nous

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



[Contactez-nous](#)



Source : *Faille de sécurité : Samsung conseille d'effacer les empreintes enregistrées – L'Express L'Expansion*

---

# La police utilise les



# empreintes des cadavres pour débloquent les iPhone

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

x

x

x

x

x

x

x

La police utilise les empreintes des cadavres pour débloquent les iPhone

**Plusieurs sources dans les autorités policières américaines ont admis à Forbes utiliser les empreintes des corps pour débloquer les iPhone grâce au Touch ID, dans le cadre d'une enquête criminelle.**

La police cherche maintenant à savoir comment ils peuvent utiliser la reconnaissance faciale Face ID pour pirater les téléphones des suspects. Bob Moledor, spécialiste judiciaire au FBI, a déclaré à Forbes que la première utilisation connue du Touch ID dans une enquête criminelle remonte à 2016, après l'attaque terroriste dans l'université d'Etat de l'Ohio d'Abdul Razak Ali Artan, abattu ensuite par un policier. Moledor a confirmé qu'un agent du FBI a placé l'index du décédé sur son iPhone dans le but d'accéder à son téléphone et de révéler davantage d'informations sur ses motivations. Malheureusement, la tentative a été infructueuse car, pendant que le FBI demandait l'autorisation pour accéder au téléphone, il s'est éteint, ce qui signifie qu'un code était également nécessaire...[lire la suite]

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, twitter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à se mettre en conformité avec la réglementation numérique (dont le RGPD) et à se protéger des pirates informatiques.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)
- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS
  - RECHERCHE DE PREUVES
- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.

Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité **RGPD** ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la **cybercriminalité** (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

**Le Net Expert**  
**INFORMATIQUE**  
Consultant en Cybercriminalité et en  
Protection des Données Personnelles

Contactez-nous



Source : *La police utilise les empreintes des cadavres pour débloquer les iPhone*

---

## **Alerte Android : Le pire ransomware jamais détecté fait ses premières victimes**

✕	<b>Alerte Android : Le pire ransomware jamais détecté fait ses premières victimes</b>
---	---

---

Android est à nouveau visé par un malware vendredi 13 octobre : DoubleLocker, un redoutable ransomware, chiffre les fichiers sur le smartphone et change son mot de passe, même s'il n'est pas rooté. Des chercheurs de ESET à l'origine de la découverte expliquent que ce ransomware se cache dans un APK d'Adobe Flash Player ce qui peut augmenter le risque d'une propagation rapide. La seule façon de s'en débarrasser c'est de réinitialiser le smartphone. Ce serait le pire ransomware détecté à ce jour.

Les chercheurs de ESET viennent de découvrir le premier ransomware Android capable de prendre le contrôle total de votre smartphone. Il parvient à obtenir des droits administrateur même sur des smartphone non-rootés, ce qui le rend extrêmement dangereux. Android/DoubleLocker.A est basé sur un trojan bancaire modifié pour changer le code PIN du smartphone sur lequel il est installé et chiffrer ses données. Les chercheurs précisent qu'un tel mode d'action était jusqu'ici du jamais vu.

## Android : le pire ransomware jamais détecté, DoubleLocker, bloque et chiffre les smartphones

Le chercheur Lukáš Štefanko à l'origine de la découverte de DoubleLocker ajoute : « à cause du fait qu'il trouve son origine dans un malware bancaire, DoubleLocker pourrait très bien être modifié pour devenir ce que l'on pourrait appeler un malware bancaire-rançon. Un malware à deux étages, qui essaie d'abord de voler vos données bancaires et/ou vider votre compte ou compte PayPal, puis bloque votre appareil et ses données pour exiger une rançon... spéculation de côté, on a détecté la version test d'un tel malware dans la nature pratiquement en même temps, en mai 2017 ». On trouve DoubleLocker dans des APK de Flash Player sur de sites compromis méthode déjà utilisée par d'autres malwares. Une fois lancée, l'application lance un service d'accessibilité baptisé Google Play Service. Le malware obtient ensuite tout seul les permissions d'accessibilité, puis les utilise pour activer les droits administrateurs et se définir comme Launcher par défaut. Dès que l'utilisateur appuie sur le bouton Home, le malware est activé. Le PIN est alors changé et les fichiers du répertoire principal chiffrés. Le ransomware demande alors de payer 0.013 BTC dans les 24 heures, soit environ 62 euros au moment où nous écrivons ces lignes. Les chercheurs relèvent que les fichiers chiffrés, qui prennent l'extension .cryeye, ne sont pas supprimés à l'issue de ce délai...[lire la suite]

---

QUE PROPOSE LE NET EXPERT, (EXPERT INFORMATIQUE ASSERMÉNTÉ) :

- SENSIBILISATIONS / FORMATIONS (n° formateur)
  - RECHERCHE DE PREUVES
- EXPERTISES & AUDITS (certifié ISO 27005)  
NOTRE MÉTIER :
  - SENSIBILISATION / FORMATIONS :
    - CYBERCRIMINALITÉ
    - PROTECTION DES DONNÉES PERSONNELLES
      - AU RGPD
      - À LA FONCTION DE DPO
  - RECHERCHE DE PREUVES (outils Gendarmerie/Police)
    - ORDINATEURS (Photos / E-mails / Fichiers)
    - TÉLÉPHONES (récupération de Photos / SMS)
      - SYSTÈMES NUMÉRIQUES
  - EXPERTISES & AUDITS (certifié ISO 27005)
    - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
      - SÉCURITÉ INFORMATIQUE
      - SYSTÈMES DE VOTES ÉLECTRONIQUES

**FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO** : En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, suivez nos formations ;

**COLLECTE & RECHERCHE DE PREUVES** : Nous mettrons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

**EXPERTISES TECHNIQUES** : Dans le but de prouver un dysfonctionnement, de déposer ou vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense ;

**AUDITS RGPD / AUDIT SÉCURITÉ / ANALYSE D'IMPACT** : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des nombreuses formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration et vous accompagnons dans l'établissement d'une analyse d'impact et de votre mise en conformité ;

**MISE EN CONFORMITÉ CNIL/RGPD** : Nous mettrons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assisterons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

**Besoin d'un Expert ? contactez-nous**

**NOS FORMATIONS** : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>  
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : Android : le pire ransomware jamais détecté fait ses

# Comment pirater un téléphone sans le toucher ?

✖	Comment pirater un téléphone sans le toucher ?
---	--

---

**L'exploitation de failles de sécurité se trouvant au niveau du protocole Bluetooth permet de pirater un appareil à distance. La démonstration est faite sur un smartphone Android, mais les vulnérabilités concernent potentiellement d'autres types d'appareils.**

Armis, entreprise spécialiste des questions de sécurité informatique, a découvert huit exploits (ces éléments de programme visant à exploiter une faille informatique) réunis sous l'étiquette BlueBorne, et permettant de prendre à distance le contrôle de téléphones, d'objets connectés et même potentiellement d'ordinateurs. « *Nous nous attendons à découvrir beaucoup d'autres vulnérabilités de ce type sur diverses plateformes proposant une connexion Bluetooth. Ces failles sont actuellement ouvertes, et peuvent être exploitées par les hackers. Les attaques via BlueBorne peuvent être utilisées pour réaliser tout un arsenal de piratages différents, autorisant l'exécution de code malveillant à distance ou encore la prise de contrôle des appareils* », explique Armis...[lire la suite]

---

## **NOTRE MÉTIER :**

- **FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO**
- **EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES**
- **AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT**
  - **MISE EN CONFORMITE RGPD / FORMATION DPO**

**FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO** : En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, découvrez nos formations ;

**EXPERTISES TECHNIQUES** : Pour prouver un dysfonctionnement, dans le but de déposer plainte ou de vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense ;

**COLLECTE & RECHERCHE DE PREUVES** : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

**AUDITS RGPD / AUDIT SÉCURITÉ / ANALYSE D'IMPACT** : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

**MISE EN CONFORMITÉ CNIL/RGPD** : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

**Besoin d'un Expert ? contactez-nous**

### **NOS FORMATIONS**

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>  
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *BlueBorne : le hack qui permet de pirater un téléphone sans le toucher*

---

**Alerte : Facebook Messenger  
pourrait propager un virus**

	<b>Alerte : Facebook Messenger pourrait propager un virus</b>
---	---

---

**Les applications de messageries instantanées sont souvent la cible de virus informatiques. Facebook Messenger n'a pas échappé à cette règle: selon Le Monde Informatique, un logiciel malveillant (« malware », ndlr) se propage actuellement sur le réseau social.**

C'est le chercheur David Jacoby, de la société informatique spécialisée dans la sécurité des systèmes d'information, qui a pu détecter ce virus. Le principe est classique: un de vos contacts envoie une vidéo nommée « David Video ». David Jacoby précise au *Monde Informatique*: « Lorsque la victime clique sur la fausse vidéo, le malware redirige vers un éventail de sites énumérant leur navigateur, système d'exploitation et d'autres informations vitales. Selon leur OS, ils sont redirigés vers d'autres sites web ».

Ce virus, qui ne menace pas l'appareil en lui-même, peut installer des logiciels malveillants à l'insu de l'utilisateur. En outre, il peut également récupérer les données personnelles...[lire la suite]

---

## **NOTRE MÉTIER :**

**EXPERTISES / COLLECTE & RECHERCHE DE PREUVES** : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

**PRÉVENTION** : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

**SUPERVISION** : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

**AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT** : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

**MISE EN CONFORMITÉ CNIL/RGPD** : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

**Besoin d'un Expert ? contactez-vous**

### **NOS FORMATIONS**

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>  
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Un virus informatique détecté sur Facebook Messenger*

---



# Plus de 100 000 smartphones Android infectés par un botnet DDoS



## Plus de 100 000 smartphones Android infectés par un botnet DDoS

**Les victimes étaient infectées par des centaines d'applications en apparence inoffensives, diffusées par le Google Play Store.**

On ne cesse de le répéter : attention aux applications que vous téléchargez, y compris sur le Google Play Store. Des chercheurs en sécurité viennent de démanteler WireX, un botnet spécialisé en attaques par déni de service distribuées (DDoS) et qui regroupait jusqu'à 120.000 smartphones zombies répartis dans plus de 100 pays. Ce n'est pas la première fois qu'un tel botnet est détecté. En septembre 2016, les chercheurs d'Imperva avait déjà mis le doigt sur un réseau de smartphones Android zombies destiné au DDoS et composé de plus de 26.000 nœuds...[lire la suite]

### **NOTRE MÉTIER :**

**EXPERTISES / COLLECTE & RECHERCHE DE PREUVES** : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

**PRÉVENTION** : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

**SUPERVISION** : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

**AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT** : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

**MISE EN CONFORMITÉ CNIL/RGPD** : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

**Besoin d'un Expert ? contactez-vous**

### **NOS FORMATIONS**

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>  
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Plus de 100 000 smartphones Android esclaves d'un botnet DDoS*

---

# Attention à Faketoken, le malware Android qui vole les données bancaires en copiant des applis

✕	<b>Attention à Faketoken, le malware Android qui vole les données bancaires en copiant des applis</b>
---	---

---

**Une version améliorée d'un cheval de Troie bancaire vieux d'un an a été repérée par des chercheurs en sécurité en Russie.**

Pour la firme de sécurité Kaspersky les malwares bancaires sont l'une des plus grandes menaces qui pèsent sur les smartphones Android. L'un d'eux, Faketoken, connu depuis un an environ, est de retour sous une nouvelle forme plus dangereuse, prévient-elle.

Au départ, ce cheval de Troie interceptait des SMS pour y récupérer des données bancaires que des utilisateurs imprudents auraient pu y indiquer. Désormais, il se greffe directement sur des applis bancaires ou sur des applis de réservations de taxis, de VTC ou d'hôtels afin de faire la même opération et écoute vos appels.

Comment parvient-il à infecter un smartphone ? Grâce à l'envoi en masse de SMS proposant de télécharger des photos. Dès lors qu'un utilisateur clique sur le lien, le malware s'installe discrètement sur l'appareil...[lire la suite]

## **NOTRE MÉTIER :**

**EXPERTISES / COLLECTE & RECHERCHE DE PREUVES** : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

**PRÉVENTION** : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

**SUPERVISION** : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

**AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT** : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

**MISE EN CONFORMITÉ CNIL/RGPD** : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

**Besoin d'un Expert ? contactez-vous**

### **NOS FORMATIONS**


: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>  
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Faketoken, le malware qui vole les données bancaires en copiant des applis*

**Mettez à jour votre téléphone sous Android. 101 failles dont 27 critiques à corriger**

	<b>Mettez à jour votre téléphone sous Android. 101 failles dont 27 critiques à corriger</b>
---	---

---

**Plus d'une centaine de vulnérabilités sont retirées d'Android. Dont de nombreuses liées aux puces de l'américain Qualcomm.**

**Google** vient de publier le bulletin de sécurité de juin concernant le système d'exploitation mobile **Android** (en moutures 4.4, 5.0, 5.1, 6.0, 7.0 et 7.1).

Au menu, la correction de **101** failles de sécurité, dont **27** sont considérées comme critiques. Ces dernières permettent potentiellement la prise de contrôle du téléphone par une application malveillante.

La plupart de ces failles critiques touchent le code livré par **Qualcomm** pour ses puces. Le concepteur américain de SoC ARM montre ici sa capacité à proposer un bon « service après-vente » logiciel. Avec une amélioration constante des pilotes et applicatifs liés à ses offres.

## **Mise à jour au bon vouloir des constructeurs**

Bien évidemment, il est vivement conseillé d'installer cette mise à jour d'Android rapidement. À condition bien entendu que votre constructeur de smartphone la relaie. Pas de souci à attendre du côté des terminaux mobiles distribués par Google. Les **Nexus** 5X, 6, 6P, 9, Player, ainsi que les **Pixel**, C et XL ont en effet déjà eu droit à cet update...[lire la suite]

---

**Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

**Source : *Google corrige 101 failles d'Android, dont 27 critiques***