

Bitdefender : : Etes-vous plus espionné sur Android ou sur iOS ?

Sécurité

Posté par : JerryG

Publié le : 12/7/2013 14:00:00

Bitdefender publie les résultats d'une analyse menée sur les **comportements les plus intrusifs des applications Android et iOS**. Bitdefender, après avoir analysé plusieurs centaines de milliers d'applications, révèle que celles-ci sont tout aussi intrusives et indiscrètes sous iOS que sous Android.

Alors que l'on pourrait penser l'un des deux systèmes d'exploitation plus intrusif que l'autre, il résulte que les données personnelles des utilisateurs d'appareils mobiles (contacts, adresses e-mail, localisation, etc.) sont aussi bien en danger sous Android que sous iOS.

Depuis près d'un an, Bitdefender analyse des applications gratuites disponibles sur Google-Play et l'Apple Store pour y déceler les comportements les plus intrusifs. Grâce à l'outil Clueful, développé et mis à disposition gratuitement par Bitdefender, le nombre d'applications analysées s'élève à 314 474 applications pour Android et 207 843 pour iOS.



Télécharger la version Premium

Clueful pour Android

Sachez ce que font vos applications

Bitdefender Clueful pour Android est une solution GRATUITE qui vous informe sur ce qu'elles font de vos données privées.

- ✓ Analyse complète
- ✓ Protège à l'installation
- ✓ Calculateur de Score de vie privée
- ✓ Complètement gratuite



Bitdefender Clueful permet de savoir quelles sont les applications mobiles qui tentent d'accéder à vos données personnelles et comment sont gérées ces informations, théoriquement privées, qui transitent sur Internet.

Parmi ces comportements intrusifs et indiscrets, parfois intégrés par les développeurs d'applications eux-mêmes, l'attitude de Bitdefender révèle le que :

45,41 % des applications iOS intègrent des services de localisation contre 34,55 % sous Android. Avec une implantation et des formes d'utilisation similaires sur les deux plates-formes, ces espions sont souvent demandés par les publicitaires et intégrés via des composants API (framework APIs) pour connaître les habitudes des utilisateurs.

À ce stade de l'attitude, seulement 7,69% des applications Android peuvent accéder à votre liste de contacts alors que les applications iOS se montrent davantage indiscrettes :

18,92 % sont techniquement capables de lire vos contacts.

14,58 % des applications Android peuvent divulguer l'identifiant de votre appareil et 5,73 % transmettre votre adresse e-mail. De nouveau, les applications iOS semblent recueillir plus de données personnelles que celles conçues pour Android. Là aussi, ces informations sont très intéressantes pour les réseaux publicitaires et sont susceptibles d'être partagées ou revendues à des tiers pour, par exemple, l'envoi de publicités ciblées en fonction du comportement et du profil des utilisateurs.

8,82 % des applications Android analysées par Clueful peuvent divulguer les numéros de téléphone d'un appareil à des publicitaires. Les applications intégrant Air Push et parfois LeaBolt permettent aux développeurs de recueillir, crypter et d'envoyer le numéro de téléphone à l'insu des utilisateurs.

Si la géolocalisation, l'accès aux contacts de l'appareil ou l'interaction avec les réseaux sociaux, peuvent être légitimes pour certaines fonctionnalités, ces comportements deviennent intrusifs lorsque les données personnelles de l'utilisateur ne sont pas indispensables au bon fonctionnement des applications mais collectées pour être monétisées par les développeurs. En d'autres termes, l'application ne devient gratuite qu'une fois payée par l'utilisateur avec ses données personnelles.

La situation est même pire, puisque payer l'application n'assure pas à l'utilisateur que ses données privées ne soient plus collectées ni même rendues à son propriétaire puisque déjà stockées dans des fichiers. De plus, la collecte de ces données est faite sans que l'utilisateur ait connaissance des autorisations accordées lors de l'installation de l'application.

Que ce soit au moment de l'installation de l'application Android ou lors de son exécution pour une application iOS, l'utilisateur devrait lire attentivement les autorisations demandées. Grâce à l'outil gratuit Clueful de Bitdefender, il peut aussi s'informer sur les risques d'atteinte à sa vie privée et ainsi se prémunir contre d'éventuels usages non désirés de ses informations personnelles.

L'attitude Bitdefender sur les comportements intrusifs des applications Android et iOS est disponible ici

[Bitdefender Clueful pour Android est disponible gratuitement ici et sur Google Play.](#)

[Pour la version iOS.](#)

[Pour retrouver Bitdefender en ligne](#)