

## Des logiciels espions chinois installés naïvement sur des Androïds ? Le scandale qui touche 700 millions de smartphones dans le monde



Au moins 120 000 téléphones (mais peut-être beaucoup plus...), envoient des données extrêmement précises, comme la géolocalisation et le contenu des messages, à des serveurs en Chine.

Avec Atlantico.fr

La révélation est une bombe. On savait depuis longtemps les problèmes de sécurité sur les smartphones, et le problème de hacking depuis, notamment, la Chine et la Russie. Mais cela va au-delà de ce qu'on avait vu jusqu'à présent.

### Le scandale

De nombreux smartphones utilisant le logiciel Android (la plupart du temps des appareils de premier prix) disposaient d'un logiciel qui envoie, toutes les 72 heures, l'historique de la géolocalisation, mais aussi des appels, et tous les SMS de l'utilisateur vers un serveur en Chine, [a révélé le New York Times](#). Le logiciel pouvait également reprogrammer à distance le téléphone de l'utilisateur pour en prendre le contrôle et, par exemple, installer des applications sans que l'utilisateur ne consente ou ne puisse l'arrêter, [précise le site spécialisé Ars Technica](#).

Le logiciel, de l'entreprise chinoise Shanghai Adups Technology Company, fonctionne ainsi intentionnellement. Il est préinstallé sur les téléphones et les utilisateurs ne peuvent pas en découvrir l'utilisation ou l'arrêter. Il ne s'agit pas d'un bug ou d'une faille de sécurité explique Tom Karygiannis, vice-président de Kryptowire, la société qui a découvert le logiciel, [au site spécialisé The Verge](#).

Pour l'instant, on ne sait pas combien de téléphones ont cette "fonctionnalité". La société Adups déclare que ses logiciels sont installés sur plus de 700 millions de téléphones, voitures et autres appareils intelligents. Un fabricant américain, BLU Products, a déclaré que 120 000 de ses téléphones étaient affectés et qu'il avait mis à jour le logiciel pour éliminer le transfert de données.

La société Kryptowire a découvert la fonctionnalité par hasard, après qu'un de ses ingénieurs a acheté un téléphone affecté pour un voyage à l'étranger et qu'il découvre des transferts de données inhabituels. La société a d'abord transmis sa découverte au gouvernement américain, puis l'a publiée ce mardi.

On ne sait pas à quelles fins le logiciel fonctionnait. Il y a deux possibilités évidentes : le ciblage publicitaire, ou l'espionnage.

"Il s'agit d'une entreprise privée qui a fait une erreur", a déclaré Lily Lim, avocat californien qui représente la société chinoise, rajoutant que la société n'est pas affiliée au gouvernement chinois.

### En pratique ?...

---

Voici la version des faits de la société Adups : la société a créé ce logiciel à la demande d'un fabricant de téléphones chinois, qui voulait stocker les données à des fins de service client, pour identifier les appels et messages mal intentionnés. Il s'agissait uniquement d'une fonctionnalité pour le marché chinois et c'est par erreur que la société l'a installé sur des téléphones pour le marché international.

Qui est concerné ? Et que faire ? Jusqu'à présent, impossible de le savoir vraiment. Adups n'a toujours pas publié de liste des modèles de téléphone qui ont cette fonctionnalité. Mais il semblerait qu'il s'agit presque exclusivement de téléphones pré-payés de premier prix.

Android étant un système d'exploitation "open source" que n'importe qui peut utiliser à ses fins, de nombreux fabricants et opérateurs peuvent créer leurs propres versions, y compris éventuellement avec des logiciels malveillants. Des sociétés comme Apple et BlackBerry auront beau jeu de signaler que leurs plate-formes sont contrôlées et que leurs systèmes de messagerie — iMessage et BBM, respectivement — sont cryptées.

Avec des bonnes compétences techniques, on "pourrait" découvrir si son téléphone est vulnérable, explique Karygiannis. "Mais le consommateur moyen ? Non."