Le hack étonnant qui peut tromper Siri, Cortana et Google Now grâce aux ondes radio | Le Net Expert Informatique

	Le hack étonnant qui peut tromper Siri, Cortana et Google Now grâce aux ondes radio

Deux hackers français ont montré qu'il était possible d'injecter des commandes vocales par l'émission d'ondes radioélectriques. Mais cette attaque nécessite quand même un peu de matériel.

Les assistants vocaux sont bien pratiques et déployés sur pratiquement tous les smartphones aujourd'hui, qu'il s'agisse de Siri pour iOS, de Google Voice pour Android ou de Cortana pour Windows 10 Mobile. Mais ces interfaces présentent des vulnérabilités que deux chercheurs en sécurité de l'ANSSI – José Lopes Esteves et Chaouki Kasmi – ont mis en lumière dans un article publié par le magazine scientifique IEEE Electromagnetic Compatibility. Ils ont également présenté leurs recherches en juin dernier, à l'occasion de la conférence académique SSTIC, qui s'était déroulée à Rennes.

Les deux chercheurs ont montré qu'il était possible d'injecter des commandes vocales dans ces systèmes par l'intermédiaire d'ondes radio. Comment? Au travers des écouteurs du kit mains-libres. « Le câble des écouteurs est une bonne antenne pour des fréquences comprises entre 80 et 108 MHz », explique José Lopez Esteves, dans la vidéo de leur présentation SSTIC. L'idée du hack est donc d'enregistrer une commande vocale, de la moduler en amplitude sur une onde porteuse de la bande 80-108 MHz et de l'envoyer vers les écouteurs. Ce rayonnement va induire dans le câble un signal électrique qui va automatiquement être traité par le système de commandes vocales, après avoir été filtré et amplifié. Au final, « on obtient un signal relativement proche du signal vocal original », précise M. Lopes Esteves.

Cette attaque fonctionne avec tous les principaux systèmes vocaux disponibles, à savoir Cortana, Siri et Google Voice. Il y a néanmoins une condition nécessaire, c'est que la commande vocale soit activée, c'est-à-dire que l'on puisse interroger l'assistant virtuel par un simple mot-clé (« OK Google », « Dis Siri » ou « Hey Cortana »), ce qui n'est pas une option par défaut sur les smartphones.

L'impact de l'attaque dépendra de l'état du téléphone. Il sera maximal s'il est déverrouillé. L'assistant vocal pourra alors accéder au carnet d'adresse, envoyer un message, ouvrir une page web, lancer une application, etc. « On pourra par exemple envoyer une commande pour que l'appareil ouvre un site web malveillant », souligne M. Lopes Esteves. Le mieux dans cette affaire, c'est que l'utilisateur pourrait ne rien remarquer du tout car la commande vocale injectée est totalement silencieuse pour lui. Seul l'assistant vocal l'entendra.

Limité à quelques mètres

En revanche, si le téléphone est verrouillé, l'assistant vocal n'aura qu'un accès limité, comme par exemple interroger l'appli météo ou appeler un numéro. Ce qui n'est pas rien quand même, car il est possible alors de passer des coups de fil en douce pour générer des revenus frauduleux (via des numéros surtaxés) ou pour simplement espionner les conversations environnantes.

Si ce piratage est relativement simple sur le principe, il nécessite quand même du matériel. Avec un équipement radio de la taille d'un sac à dos, le rayon d'action est de seulement deux mètres. Pour atteindre cinq mètres, il faut déjà une camionnette. Et dans ce cas, mieux vaut ne pas se trouver à proximité de l'émetteur, car le niveau de rayonnement sera alors plutôt intense.

Source :
http://www.01net.com/actualites/siri-cortana-et-google-voice-sont-vulnerables-aux-attaques-radio-922670.html
Par Gilbert KALLENBORN