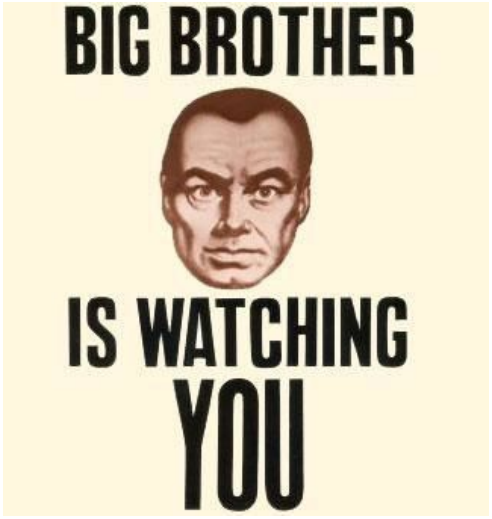
Alerte Faille Android ! Big Brother pourrait bien vous surveiller | Le Net Expert Informatique

	Alerte Faille Android ! Big Brother pourrait bien vous surveiller

Des chercheurs en sécurité ont récemment découvert une faille de sécurité considérée comme la pire jamais découverte dans le système Android. Détecté dans la bibliothèque multimédia de l'OS, ce bug nommé « Stagefright » expose près d'1 milliard de terminaux Android aux malwares.

En exploitant la faille « Stagefright », les hackers peuvent accéder aux contacts et aux autres données stockées dans un appareil mobile telles que les photos et les vidéos. Ils peuvent également accéder au microphone et à la caméra de cet appareil, ce qui leur permet d'espionner l'utilisateur via l'enregistrement de son et la prise d'images.

Tous les appareils exécutant des versions Android 2.2 Froyo jusqu'aux versions 5.1.1 Lollipop sont concernés. Cela représente environ 95% de l'ensemble des terminaux Android.

Le plus effrayant, c'est que les pirates ont uniquement besoin du numéro de téléphone de l'utilisateur pour infecter son appareil. Le malware est transmis lors de l'envoi d'un message multimédia à n'importe quelle application de messagerie pouvant traiter les formats vidéo MPEG4, telle que l'application de messagerie par défaut de l'appareil Android, Google Hangouts ou Whatsapp. Comme ces applications de messagerie Android récupèrent automatiquement des vidéos ou du contenu audio, le code malveillant est exécuté sans que l'utilisateur n'ait besoin de faire quoi que ce soit. En effet, la faille n'exige pas que la victime ouvre le message ou clique sur un lien. Il s'agit d'un malware unique en son genre car ce type de menace nécessite généralement une action de la part de l'utilisateur pour que l'appareil soit infecté. Il pourrait par exemple être relayé via un lien envoyé par courrier électronique ou partagé sur les réseaux sociaux. Toutefois, cela nécessiterait encore et toujours une action de la part de l'utilisateur, puisque le chargement d'une vidéo se fait uniquement via l'ouverture d'un lien. Cela est extrêmement dangereux, car si les utilisateurs sont infectés via MMS, aucune action ne leur sera demandée et les effets indésirables seront imperceptibles. Avant même que les victimes s'en aperçoivent, le hacker est en mesure d'exécuter le code et de retirer toute trace attestant que l'appareil a été infecté.

Le rêve du cybercriminel et du dictateur

Les cybercriminels profitent de cette faille de sécurité pour espionner des millions de personnes et exécuter d'autres codes malveillants. Les gouvernements répressifs pourraient abuser de ce bug en vue d'espionner leurs citoyens ou leurs ennemis. Toutefois, ce bug pourrait également être utilisé à des fins d'espionnage apolitique. Les pirates peuvent facilement surveiller les personnes de leur entourage comme leur conjoint ou leurs voisins. Ils n'ont besoin pour ce faire que du numéro de téléphone de la personne visée. Les hackers ont aussi la possibilité de dérober des informations personnelles qu'ils utiliseront pour faire chanter des millions de personnes ou usurper leur identité. Les conséquences possibles de ce type de faille sont donc à prendre au sérieux.

Une nécessité urgente de patchs

Des patchs complets doivent désormais être fournis par les fabricants de téléphones à l'aide d'une mise à jour à distance ou « over-the-air » (OTA) d'un firmware pour les versions Android 2.2 et plus. Malheureusement, les mises à jour pour appareils Android ont toujours mis beaucoup de temps pour arriver jusqu'à l'utilisateur final. Espérons que les constructeurs réagiront plus rapidement dans ce cas précis.

Google y a pour sa part déjà répondu d'après un témoignage d'HTC publié dans le magazine d'information hebdomadaire américain Time : « Google a informé HTC de cette problématique et fourni les patchs nécessaires qu'HTC a commencé à prendre en compte dans les projets mis en œuvre au début du mois de juillet. Tous les projets en cours contiennent le patch requis. » Pour le moment et par mesure de précaution, il est recommandé aux utilisateurs de désactiver la fonction récupération automatique des MMS dans les paramètres par défaut de l'application de messagerie.

Source : http://www.journaldun
et.com/solutions/expert/61932/big-brother-po
urrait-bien-vous-surveiller-grace-a-la-faille-stagefright.shtml
Par Filip Chytrý