GSMem : Pirater un PC sans connexion via le réseau GSM

Un pas de plus est franchi dans la mise en défaut des ordinateurs en mode « air gap » c'est-à-dire complétement isolé de toutes connexions et protéger sur le plan électromagnétique. Une équipe de chercheurs du centre de recherches Ben Gourion de l'Université du Negev a réalisé un POC (proof of concept) montrant le piratage d'un tel système en utilisant les fréquences GSM et un téléphone mobile bas de gamme. Cette méthode va être présentée à l'occasion de la conférence Usenix qui se déroulera à Washington du 12 au 14 août prochain. Nos confrères de Wired ont pu néanmoins avoir quelques éléments supplémentaires.

Elle repose sur la création **d'un malware nommé GSMem**. Il exploite les ondes électromagnétiques et **force le bus mémoire** de l'ordinateur à fonctionner comme une antenne pour des données à un téléphone via le réseau cellulaire. Il s'appuie sur l'architecture multicanal de la mémoire pour amplifier le signal. Le malware fonctionne en complément d'un rootkit mobile embarqué dans la puces radio d'un téléphone. Le rootkit peut être installé via de l'ingénierie sociale, un accès physique ou une application malveillante. La puce peut alors gérer la connexion entre le réseau GSM et les basses fréquences du PC.

Un siphonnage de mot de passe à 30 mètres

Le malware est plus difficile à installer sur l'ordinateur cible, car par essence il est isolé du réseau public. Il faut en général un accès physique ou injecter le malware dès la chaîne de montage. Dans le test, il a été implanté sur trois configurations, Windows, Ubuntu et une autre distribution Linux. Une fois le malware installé sur l'ordinateur (il ne représente que 4 Ko), les données peuvent être reçues à **une distance de 1 à 6 mètres** (cf vidéo ci-dessous). Avec une antenne plus puissante, la réception peut se faire sur une distance de 30 mètres. Le débit est relativement faible entre **1 à 2 bits par seconde** et la taille des données exfiltrées reste modeste. Mais c'est suffisant pour obtenir des mots de passe ou une clé de chiffrement en une minute ou deux.

Les chercheurs se sont appuyés sur d'anciens travaux relatifs au piratage des ordinateurs air gap. Mais la particularité de leurs travaux est de s'être focalisé sur les fréquences GSM et d'avoir utilisé un vieux téléphone. Pour la démonstration, ils ont pris un **Motorola C123** vieux de 9 ans qui ne dispose que de la connectivité 2G (pas de WiFi, ni Edge ou GPRS). Avec cette démonstration, les spécialistes veulent sensibiliser les responsables des sites sensibles ou critiques dans lesquels on trouve ce type d'ordinateur. Les smartphones sont en général interdits du fait de leur connectivité et des possibilités de prendre des photos ou des vidéos. Par contre, les mobiles d'entrée de gamme restent autorisés. Il faudra peut-être revoir sa copie !

A lire aussi :

Le GSM bientôt au service de la 4G en France ?
Hacker des ordinateurs avec la chaleur des composants