Black Hat : Transformer les objets connectés en radio espion

Utiliser des appareils informatiques pour envoyer des informations par signal radio à l'extérieur des murs de l'entreprise. Tel est l'objet de la démonstration qu'a faite **Ang Cui**, doctorant à l'université Columbia, à l'occasion de la Black 2015 de Las Vegas. Ce chercheur spécialisé dans la détection d'intrusion a montré comment il était possible de détourner des appareils aussi courants que des imprimantes, disques durs et une foule de systèmes électroniques connectés pour en faire des émetteurs radio. Il suffit alors de capter ce signal radio pour recueillir les données qu'elles émettent.

Faire vibrer les broches pour émettre des ondes

Mais comment transformer une imprimante en radio ? Simplement en allumant et éteignant suffisamment rapidement les broches de connexion d'Entrées/Sorties d'un composant électronique ce qui a pour effet de générer une onde, sonore ou pas selon la fréquence, suffisamment puissante pour traverser l'espace et les murs d'un bureau jusqu'à un récepteur dédié. Un simple récepteur radio portatif de base suffit pour capter le signal, a précisé le chercheur qui a baptisé son système de « **Funtenna** ».

Plus exactement, c'est la manipulation des composants **UART** (attached universal asynchronous receiver/transmitter) qui permet de faire vibrer les connecteurs et générer un signal radio. Configurables, les *chips* UART sont chargés de transcrire les données séries en données parallèles. Le chercheur pense que Funtenna fonctionne avec tous types de modules UART. Pour la démonstration, Ang Cui a utilisé **une imprimante de marque Pantum** à laquelle il a envoyé un message simple (une phrase extraite du roman *Neuromancer* de William Gibson) encodée en binaire (0 et 1) et dont il a exploité le câble connectée aux broches UART comme antenne pour émettre le signal. Mais le scientifique estime que le principe fonctionnerait avec n'importe quel appareil peu sécurisé, lesquels composent la plupart des objets connectés aujourd'hui.

Deux obstacles majeurs

Ang Cui reconnaît néanmoins deux obstacles majeurs à la mise en œuvre de Funtenna : installer **un appareil chargé de formater les données** à envoyer à « l'émetteur radio » (l'imprimante dans le cas présent); et **être suffisamment proche** avec le récepteur pour capter les ondes émises par l'appareil émetteur. Probablement un jeu d'enfant pour les services d'espionnage.

Le Funtenna n'est pas le premier système à s'appuyer sur les ondes émises par les appareils électroniques pour capter les données qu'ils transportent. Lesquelles sont rarement prises en compte dans un système de sécurité d'entreprise. Néanmoins, Funtenna confirme à sa manière l'existence possible de cette forme de piratage, voire en montre la simplification. Du moins quand Ang Cui en aura apporter la preuve de concept afin de permettre aux autres chercheurs et firmes de sécurité de vérifier et confirmer ses travaux. Ce qu'il a promis de faire après le Black Hat.

Lire également

Black Hat : les carte SIM 3G/4G craquées en 10 minutes

32 failles zero day dévoilées à la prochaine Black Hat USA

L'attaque Man In The Cloud se joue des services de stockage Cloud

crédit photo © fotographic1980 – shutterstock