Des modems 4G Huawei exposent des PC portables aux pirates

A l'occasion de la 23e édition de la Def Con, qui se tenait du 6 au 9 août à Las Vegas, Mickey Shkatov et Jesse Michael d'Intel Security Group (ex-McAfee) ont révélé comment une faille dans un modem sans fil pouvait servir à maintenir un accès persistant à un terminal. Lors de leur conférence «Scared Poopless – LTE and *your* laptop», les deux chercheurs en sécurité ont mis en évidence des failles d'un modem LTE/3G/2G qui permettent de remplacer son firmware d'origine par un microgiciel infectieux.

Utilisé dans bon nombre de PC portables d'entreprise sous Windows et de tablettes, le module Huawei ME906 opère son propre système (une version modifié d'Android), indépendamment de l'OS hôte. Un système indépendant qui ne dispose pas de mécanisme de validation/autorisation par signature chiffrée pour autoriser une éventuelle mise à jour. Cette absence de barrière de sécurité ouvre la possibilité de distribuer une image infectieuse du firmware par les services de mise à jour de l'OS (comme Windows Update), de la faire installer depuis un malware préinstallé sur la machine, ou encore de convaincre son utilisateur d'effectuer lui-même la mise à jour.

Un malware persistant

Connecté en interface USB au reste du système, le modem peut, potentiellement, être émulé en clavier, disque dur, souris, carte réseau ou tout autre type d'appareil USB qui permettrait aux pirates d'opérer à distance sur la machine affectée.

Une fois en place dans la puce, le firmware vérolé fournit un moyen d'infecter l'OS en permanence même quand celui-ci est réinstallé. Pire, le firmware en question pourrait bloquer toute autre nouvelle mise à jour qui tenterait de déloger les agents infectieux. Seule solution pour l'utilisateur : retirer le modem LTE de la machine (ou le désactiver d'une manière ou d'une autre). Si l'opération n'est pas impossible dans le cas d'un laptop (le modem s'apparente à une carte enfichée dans un connecteur), c'est déjà plus délicat avec une tablette (ou le modem est généralement soudé sur la carte mère). Dans tous les cas, le service de connexion sans fil mobile s'en trouverait affecté.

Huawei corrige

Huawei a livré une mise à jour de son firmware (avant même le début de la conférence dédiée à la sécurité) pour combler la faille permettant l'installation d'une image non autorisée sur son modem. Le constructeur déclare ne pas avoir été informé d'une quelconque attaque qui se serait appuyée sur la vulnérabilité en question. La mise à jour du firmware et les détails de la vulnérabilité sont disponibles à partir de cette page.

Lire également :

Black Hat : Transformer les objets connectés en radio espion
Black Hat : les carte SIM 3G/4G craquées en 10 minutes
Un bug dans Android plonge les terminaux dans le coma

crédit photo © Morrowind – shutterstock