CherryBlossom, le programme de la CIA pour pirater les hotspots Wifi

WikiLeaks vient de révéler comment la CIA peut espionner des *« cibles »* en piratant les routeurs et particulièrement les points d'accès Wifi. Le site de Julian Assange a mis la main sur des documents décrivant le projet CherryBlossom au sein de l'agence du renseignement américain sur la base de travaux réalisés et mis en œuvre par le SRI International, un centre de recherche indépendant et à but non lucratif.

Malgré ses accents printaniers (CherryBlossom pouvant se traduire par Fleur de cerisier), le projet de la CIA n'a rien de poétique. L'outil se dédie plus à des activités d'espionnage et d'attaques que de création artistique (même si certain considèrent comme du grand art les usages détournés de l'informatique). Concrètement, CherryBlossom vise à compromettre les hotspot Wifi et autres appareils sans fil afin de surveiller le trafic IP qui y circule mais aussi de pénétrer les systèmes qui y sont raccordés. Et ceux-là peuvent être nombreux alors que le Wifi s'est généralisé aussi bien dans les entreprises (grandes et petites) que chez les particuliers ou les espaces publics. La flopée de documents mis en ligne par WikiLeaks, certains remontant à 2007, décrit le fonctionnement de CherryBlossom. Si rien ne dit qu'il est toujours en cours, rien ne permet de penser le contraire non plus.

Des attaques type Homme-du-milieu

Le modèle d'attaque reste relativement classique et s'inscrit dans le type Homme du milieu (Man-in-the-middle). Il nécessite l'injection d'un firmware spécialement développé pour accéder à l'interface de contrôle du routeur. Une opération facilitée alors que certains appareils autorisent cette mise à jour par les airs et ne nécessitent donc aucune connexion filaire obligeant à se rapprocher du routeur. Une fois la cible infectée, définie comme un « FlyTrap » (piège à mouche), l'appareil se connecte à un serveur de commande et contrôle (un CherryTree, Cerisier), envoi des informations relatives au statut de l'appareil et sa sécurité, et se met en attente d'une « Mission » à exécuter. Il ne reste alors plus qu'à attendre qu'un FlyTrap envoie une alerte à un serveur CherryBlossom dès qu'un utilisateur d'Internet surveillé par la CIA s'y connecte.

Derrière Mission se cache en fait un opérateur humain capable d'accéder à l'interface du routeur depuis un navigateur (« CherryWeb »). Parmi les différentes possibilités de l'outil, l'opérateur peut récupérer les contacts d'un utilisateur du hotspot Wifi (adresses e-mail, interlocuteur de messagerie instantanée), les adresses MAC (identifiants de cartes réseau) et les numéros de VoIP mais aussi copier tout le trafic qui en sort ou encore le détourner vers un proxy. Le routeur infecté peut aussi déployer un tunnel VPN vers un serveur du programme d'espionnage afin de créer des accès directs et sécurisés vers les réseaux locaux (WLAN/LAN) des cibles et, donc, potentiellement leurs terminaux.

La plupart des points d’accès Wifi concernés

Quant à savoir comment la CIA parvient à franchir la barrière de sécurité des routeurs Wifi pour réaliser la mise à jour du firmware, les méthodes ne manquent pas pour déchiffrer les mots de passe. La méthode la plus simple étant souvent d’utiliser les identifiants du constructeur laissés par défaut lors de l’installation de l’appareil. Une méthode d’autant plus efficace que, si l’on se fie aux documents s’étalant jusqu’à août 2012, nombre de routeurs sans fil ont été ainsi déployés dans la nature à cette époque. Et de 3Com à Z-Com en passant par Linksys et Cisco, Motorola et D-Link, les plus grandes marques de routeur (à l’exception notable de Netgear) étaient référencées dans le projet CherryBlossom. Même si le périmètre opérationnel de la CIA est censé s’arrêter aux frontières américaines, il est peut-être temps de changer le mot de passe de son hotspot Wifi.

Lire également
Wikileaks : les outils de hacking de la CIA seront « désarmés » avant publication
Athena de la CIA, une autre épée de Damoclès au-dessus de Windows
Marble Framework : le double jeu perfide des hackers de la CIA