900 000 boxes Internet de Deutsche Telekom mises HS par un piratage

Panne de grande envergure pour les abonnés Internet de **Deutsche Telekom**. Selon l'opérateur, **900 000** de ses clients, soit 4,5 % des 20 millions de lignes qu'il dessert, seraient touchés par un problème de connexion.

En cause, les routeurs résidentiels de marque Zyxel et Speedport dont la société équipe ses clients. Des boxes qui – comme en France – assurent la connexion Internet, la téléphonie et l'accès à la télévision. Cette panne a démarré dimanche après midi, mais semble maintenant en passe d'être résorbée.

L'ampleur du problème est difficile à évaluer. Certains n'ont connu que des perturbations de leur liaison Internet, alors que d'autres se sont retrouvés sans connexion… et donc parfois sans possibilité d'en avertir l'opérateur.

« La grande majorité de nos clients peut utiliser nos services sans restrictions et notre réseau est pleinement opérationnel, a déclaré un porte-parole de la société. *Cependant, depuis dimanche après-midi, un nombre significatif de clients a eu des problèmes : environ 900 000 clients, équipés de routeurs spécifiques. Nous ne pouvons pas exclure la possibilité que les routeurs* ***aient été ciblés par des tiers****. Actuellement, une mise à jour logicielle est fournie pour résoudre le problème. Le déploiement du logiciel a déjà commencé. Les clients doivent débrancher leur routeur pendant 30 secondes. Ensuite, lors de la réactivation du routeur, le nouveau logiciel sera automatiquement installé depuis nos serveurs. »*

Un piratage raté ?

Plus qu'une simple panne, un piratage de certains routeurs de l'opérateur est donc envisagé.

« Les attaques de ce genre ne sont pas quelque chose de nouveau : cette année, nous avons eu plusieurs rapports portant sur des milliers de routeurs infectés utilisés pour des botnets DDoS », explique **Alex Mathews**, directeur technique EMEA chez Positive Technologies, dans les colonnes de *Silicon UK*. *« Nous soupçonnons même que cette panne allemande est* ***un botnet défectueux****. Après tout, les pirates informatiques ne sont pas très intéressés par des routeurs non fonctionnels. Ils préfèrent en prendre le contrôle et les utiliser pour d'autres attaques. »*

L'hypothèse d'un piratage ayant mal tourné n'est donc pas à exclure. Ce ne serait pas une première. Les pirates tendent en effet à attaquer les routeurs via des outils automatiques lançant du code sur des équipements réseau mal protégés. Toutefois, ces équipements évoluent au fil des versions et peuvent ainsi présenter des différences en termes d'architecture technique, d'espace de stockage ou de mémoire de travail disponible. Menant ainsi à l'échec du piratage.

Le botnet Mirai soupçonné

Si l'hypothèse du piratage se confirme, la grande question ne sera pas donc de savoir quel impact visible cette attaque a eu, mais combien des **19,1 millions d'autres routeurs** de l'opérateur sont passés sous le contrôle de pirates sans que leur fonctionnement ait été altéré.

Les experts en sécurité penchent aussi pour une attaque via le célèbre botnet Mirai. Ce dernier est connu pour enrôler des objets connectés comme des caméras de vidéosurveillance ou des routeurs. Dans le cas de Deutsche Telekom, les routeurs ciblés disposent du port 7547 ouvert pour le fournisseur d'accès à Internet puisse gérer à distance le matériel en cas de panne ou de problème. Cette ouverture est aussi utilisée par le botnet Mirai.

À lire aussi :
Piratage de Yahoo : 1 milliard de personnes seraient concernées
Smart TV Samsung : commandes vocale ou écoutes vocales ?
Microsoft va ouvrir des datacenters anti-écoutes en Allemagne