900 000 routeurs de Deutsche Telekom infectés par un malware

	900 000 routeurs de Deutsche Telekom infectés par un malware

Deutsche Telekom a confirmé la thèse d'un malware ayant infecté plus de 900.000 de ses routeurs. Selon Flashpoint, environ 5 millions de routeurs à travers le monde seraient vulnérables à la faille exploitée par cette variante de Mirai.

Le Cert-FR alerte les utilisateurs français sur cette attaque. L'équipe rappelle ainsi que « plusieurs version du binaire malveillant sont en circulation ». Le Cert-FR recommande de changer les mots de passe par défaut, de restreindre l'accès aux outils d'administration et de désactiver « les services inutilement lancés sur les équipements exposés sur le réseau. »
Mirai se tourne vers de nouvelles cibles et la nouvelle version du ver informatique s'attaque maintenant aux routeurs. On avait déjà constaté par le passé des variantes de ce malware modifiées afin de s'attaquer à de nouveaux appareils. Mais l'attaque ayant visé Deutsche Telekom montre que les opérateurs de cette nouvelle variante entendent maintenant changer de cible et délaisser les objets connectés pour s'attaquer aux routeurs.

Comme l'explique Flashpoint dans une note de blog, la mise à disposition du code source de Mirai par son créateur a entraîné une guerre entre les cybercriminels, alors que plusieurs groupes tentaient d'utiliser Mirai pour prendre le contrôle du maximum d'objets connectés vulnérables. « L'évolution logique pour ce malware était de découpler le mécanisme d'infection de la charge utile du malware, en exploitant un nouveau vecteur d'attaque » précise ainsi Flashpoint sur son blog.
La dernière déclinaison de Mirai n'exploite donc plus simplement Telnet pour tenter de se connecter à des objets connectés en utilisant les identifiants par défaut. Selon Flashpoint, celle-ci exploite des vulnérabilités connues au sein des protocoles TR-064 et TR-069, des protocoles de maintenance utilisés par les opérateurs. C'est grâce à cette faille que les opérateurs du réseau botnet sont parvenus à infecter plus de 900.000 routeurs livrés par Deutsche Telekom à ses clients. Mais selon Flashpoint, l'opérateur allemand n'est pas le seul à devoir s'inquiéter de ce type d'attaques. Flashpoint évoque ainsi le fait que des appareils infectés ont également été détectés au Brésil et en Grande-Bretagne. Selon Flashpoint, environ 5 millions de routeurs à travers le monde sont vulnérables à cette nouvelle variante.
Reste à déterminer l'origine de l'attaque contre l'opérateur. Flashpoint précise que les administrateurs de cette variante semblent être des habitués de Mirai, puisque le nouveau malware présente plusieurs points communs (notamment des serveurs de command and control) avec des Botnets déjà identifiés lors d'attaques précédentes effectuées grâce à Mirai.
Selon le journal allemand Tagesspiegel, les soupçons se tournent vers la Russie. Dans une prise de parole, la chancelière Angela Merkel s'est refusée à confirmer cette thèse, mais précise néanmoins que de nombreuses cyberattaques ont été constatées en Europe et appelle ses citoyens à s'habituer à ce type d'attaques. Cité par la presse locale, le directeur de l'équivalent allemand de l'Anssi, le BSI, évoque de son côté « le crime organisé » à l'origine de l'attaque, mais rappelle que l'attaque n'a pas fonctionné. Le malware a bien déconnecté les routeurs des abonnés, mais celui-ci n'est pas parvenu à s'installer correctement. Plus de peur que de mal donc…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Deutsche Telekom : 5 millions de routeurs vulnérables au malware – ZDNet