Sécurité : Misfortune Cookies, une faille perdure sur des millions de routeurs

Traditionnellement dans les restaurants chinois, on vous propose des biscuits de la chance, un gâteau où est insérée une petite phrase à méditer. Mais dans le domaine de la sécurité informatique, la chance a tourné pour les routeurs Internet résidentiels et professionnels selon Checkpoint. L'éditeur a en effet trouvé une faille, baptisée **Misfortune Cookies** dans un composant de plusieurs objets connectés comme des routeurs Internet pour les particuliers (en général des box) et les PME, mais également des webcams ou de téléphones IP. Au total, près de 46 millions de terminaux ont été scannés dans 189 pays par **Checkpoint** et 12 millions ont répondu positivement. La liste des fabricants touchée est longue et comprend des acteurs comme D-Link, Huawei, TP-Link, ZTE, Zyxel, etc.

Point commun de l'ensemble de ces constructeurs, ils embarquent un composant faisant office de serveur embarqué, nommé RomPager et développé par **Allegro Software**. C'est dans ce composant que la faille se trouve. « *En lui envoyant un cookie HTTP malveillant sur un port TCP particulier, il est possible de prendre la main sur l'ensemble du terminal et de faire ce que l'on veut, redirection de flux, accéder à des documents, etc* », explique Thierry Karsenty, directeur technique de la zone EMEA chez Checkpoint.

Pour autant, la faille n'est pas inconnue de la part d'Allegro Software. Selon le fabricant elle a été **repérée en 2002 et corrigée en 2005**. Pour Thierry Karsenty, *« la recherche que nous avons mené montre que cette faille continue à être présente sur beaucoup d'objets connectés »*. Et d'ajouter que « *cette affaire pose la problématique de la politique de mise à jour de sécurité dans l'Internet des objets. Nous sommes habitués dans des environnements PC à disposer de patch relativement rapidement. Ici, cela fait 9 ans que des équipements continuent à tourner avec des firmwares de composants qui ne sont pas corrigés* ». Allegro Software a renvoyé un courrier en demandant aux constructeurs de mettre à jour RomPager avec la dernière version du firmware.

A lire aussi :

Les routeurs WiFi, de vraies passoires en matière de sécurité

Le standard WPS sur les routeurs WiFi piraté plus rapidement

Crédit Photo : Oskar Orsag-Shutterstock