Forum: Sécurité

Topic: IoT et cybersécurité

Subject: IoT et cybersécurité

Publié par: Wullfk

Contribution le : 27/06/2019 00:04:37

40 % des ménages dans le monde possèdent au moins un objet connecté, selon une étude de l'éditeur Avast et l'Université de Stanford.

https://www.datasecuritybreach.fr/iot- ... -moins-un-objet-connecte/

Citation :
Avast a analysé 83 millions d'objets connectés au sein de 16 millions de foyers à travers le monde afin de comprendre la répartition et le profil de sécurité de ces appareils, par type et par fabricant. Les résultats ont ensuite été validés par les équipes en charge de la recherche chez Avast et par l'Université de Stanford.

« Les professionnels de la sécurité ont longtemps échangé sur les problèmes associés à l'émergence de l'IoT, confie Zakir Durumeric, professeur adjoint en informatique à l'Université de Stanford. Malheureusement, ces objets sont restés cachés derrière les routeurs domestiques et nous avons eu peu de données à grande échelle sur les types d'appareils réellement déployés dans les foyers. Les informations que nous avons obtenues nous aident à mieux comprendre cette adoption croissante de l'IoT, ainsi que les différentes problématiques auxquelles les utilisateurs sont confrontés en matière de sécurité. »

../..

En France

En France, l'IoT représente 21,7 % de l'ensemble des appareils présents dans le foyer, contre 24 % pour les appareils mobiles, et 29,3 % pour les PC.

Les données de cette étude ont été collectées grâce aux utilisateurs de la solution Wi-Fi Inspector d'Avast qui analyse le réseau domestique afin d'identifier les éventuelles vulnérabilités et les problèmes de sécurité susceptibles de représenter une menace. Cette fonctionnalité vérifie l'état du réseau, les appareils connectés à celui-ci et les paramètres du routeur. Wi-Fi Inspector aide les utilisateurs à protéger leur réseau afin d'empêcher les pirates informatiques d'y accéder et d'exploiter leurs données à des fins malveillantes.

L'étude s'est intéressée à la répartition des fournisseurs d'appareils connectés au niveau mondial. Alors qu'ils sont plus de 14 000, seule une poignée domine le marché.

« L'une des conclusions principales de cette recherche est que 94 % des objets connectés ont été fabriqués par moins de 100 fournisseurs différents, et la moitié par seulement 10 d'entre eux, indique Rajarshi Gupta, Head of Artificial Intelligence, chez Avast. Cela met les fabricants dans une position unique pour garantir l'accès des consommateurs à des appareils dotés d'une protection de la vie privée et d'un niveau de sécurité élevés dès la conception. »

En durcissant les objets contre les accès non désirés, les fabricants peuvent contribuer à empêcher les hackers de compromettre ces appareils à des fins d'espionnage ou d'attaques par Déni de Service (DDoS).

D'importants cyber-risques non pris en compte

Dans le cadre de l'étude, Avast a identifié un nombre significatif d'appareils exploitant des protocoles obsolètes, parmi lesquels Telnet et FTP, à savoir 7 % de la totalité des objets connectés.

C'est également le cas pour 15 % des routeurs domestiques, véritables passerelles vers le réseau ; raison pour laquelle il s'agit d'un problème grave, car lorsque les routeurs ont des identifiants faibles, ils peuvent permettre d'accéder à d'autres périphériques et potentiellement à l'ensemble du foyer pour mener une cyberattaque.

En 2019, il y a peu de raisons pour que les objets connectés supportent le protocole Telnet. Cependant, l'étude montre que les appareils de surveillance et les routeurs prennent toujours en charge ce protocole, et qu'ils ont le profil Telnet le plus faible. Cela concorde avec certains piratages survenus par le passé, notamment le rôle de ce protocole dans les attaques sur les botnets Mirai, qui laissent penser que ces types de dispositifs sont à la fois nombreux et faciles à compromettre.