Gare, portes de prison et pipeline à la merci d'un bug des serveurs IoT

Les spécialistes de la sécurité le répètent à longueur de journée, le point faible de l'Internet des objets est la sécurité. Même les politiques américains viennent d'en prendre conscience en voulant soumettre une loi sur le sujet. Et ce n'est pas du superflu au regard des différentes interventions lors de la Black Hat, qui s'est déroulée la semaine dernière à Las Vegas.

Plus particulièrement celle de Lucas Lundgren, consultant sécurité chez IO Active. Il a découvert un bug dans les serveurs IoT. Les objets connectés dialoguent en effet avec des serveurs dédiés via un protocole de messagerie, nommé MQTT (Message Queuing Telemetry Transport). Or cette communication n'est pas protégée, explique le consultant : « *il n'y a pas de sécurité via un nom d'utilisateur ou un mot de passe* », résume-t-il. Facile dès lors de scanner le Net et de découvrir des serveurs IoT ouverts à tout vent. Le chercheur en a détecté 87 000 lors de ses travaux.

Le potentiel de cette découverte est immense et effrayant. Lucas Lundgren s'est par exemple amusé à ouvrir et fermer des portes de cellules d'une prison localisée loin de chez lui. A travers des commandes, il pouvait choisir d'ouvrir ou de fermer l'ensemble des portes ou simplement quelques unes. « *Non seulement, on peut lire les données, mais ce qui est grave, on peut aussi écrire des données via du cross-scripting et des injections SQL* », constate le spécialiste.

Centrales nucléaires, Tesla et sextoys

Parmi les autres objets connectés qu'il a testés, on retrouve des machines à électrocardiogrammes, des pompes à insuline, des téléphones mobiles, des sextoys, une Tesla. Plus surprenant dans son balayage des serveurs vulnérables, il a aussi découvert des équipements liés à de la domotique, des systèmes d'alarme, des centrales nucléaires, un accélérateur de particules et un pipeline de pétrole. Sur ce dernier, il était capable de voir le niveau de la pression au sein des tuyaux, mais également les noms d'utilisateur et les mots de passe sur le système de contrôle industriel. Dans un autre registre, il avoue avoir trouvé un serveur fonctionnant dans une gare allemande, avec la possibilité de voir les trains qui roulent, où ils se trouvent et quand ils arrivent. Une personne malintentionnée pourrait trafiquer ces données et provoquer un accident.

Lucas Lundgren ne rejette pas la faute sur le protocole MQTT. « *Le protocole n'est pas le problème. Il faut toujours utiliser du chiffrement, un nom d'utilisateur et un mot de passe sur le serveur* ». Et de conclure : « *leur sécurité est entre vos mains* ».

A lire aussi :

IoT : des millions d'objets connectés exposés à une faille de gSOAP

IoT : Kone élève sa maintenance prédictive avec IBM Watson

Crédit Photo : Visual Hunt