# AT&T, IBM, Nokia et Symantec s'unissent pour sécuriser l'IoT

Si le marché de l'Internet des objets (IoT) est, selon certains, freiné par son manque d'interopérabilité, que dire alors de la sécurité des objets connectés ? A l'instar du botnet Mirai, les objets constituent aujourd'hui une cible privilégiée des cybercriminels pour lancer des attaques DDoS massives. L'exploitation de leurs vulnérabilités fait tâche dans une industrie en pleine croissance. C'est pour tenter de répondre à cet épineux problème qu'un groupe d'acteurs vient de s'unir autour de l'IoT Cybersecurity Alliance.

Emmenée par AT&T, cette nouvelle alliance consacrée à la sécurité de l'IoT réunit à ce jour IBM, Nokia, Palo Alto Networks, Symantec et Trustonic. Opérateur, équipementier télécom, spécialistes de la sécurité et société de service, cet ensemble hétéroclite d'acteurs entend partager expertises et compétences pour barrer la route à l'insécurité grandissante issue de l'IoT. Car il y a visiblement urgence. Ainsi, AT&T constate une augmentation de 3 198% du taux d'analyse de vulnérabilités dans les objets connectés par les attaquants ces trois dernières années. Et une étude conduite par l'opérateur américain souligne que 58% des utilisateurs ne font pas confiance à la sécurité de leurs périphériques IoT.

## Un objet connecté = un point d'entrée d'une cyberattaque

*« Qu'il s'agisse d'une voiture connectée, d'un stimulateur cardiaque ou d'une cafetière, chaque périphérique connecté est un nouveau point d'entrée potentiel pour les cyberattaques*, rappelle Bill O'Hern, responsable des services de sécurité chez AT&T. *Il est devenu essentiel pour les leaders de l'industrie et les innovateurs comme ceux des membres fondateurs de cette Alliance, de travailler ensemble pour aider l'industrie à trouver des approches de sécurité plus holistiques pour l'IoT. »*

[A lire aussi : IoT : 2016, l'année du décollage]

L'Alliance entend donc à la fois informer les consommateurs et éduquer l'industrie sur les mesures à prendre pour protéger les objets dans la volonté de créer un écosystème IoT salutaire. Les actions se concentreront particulièrement sur l'étude des risques encourus par les applications IoT des secteurs verticaux, l'analyse des vulnérabilités des différentes couches applicatives et les moyens de les combler, et à rendre plus facile l'accès à la sécurisation des objets. L'initiative entend également peser plus globalement sur les normes et politiques de sécurité à l'échelle de l'industrie. Les membres de l'Alliance se disent par ailleurs convaincus que la clé de la sécurité IoT réside dans la protection de tous les périphériques tant au niveau du terminal, que du réseau, du cloud et de la couche applicative. En clair, une protection à tous les étages sinon rien. Le travail ne va pas manquer.

**Lire également**

**IoT : « Pirater un réseau Lora ? A quoi bon », plaide Objenious**
**IoT : La FTC attaque D-Link pour défauts de sécurité**
**Bientôt un label européen pour la sécurité de l'IoT ?**

**crédit photo iot sécurité © alice-photo – shutterstock**