Bientôt un label européen pour la sécurité de l'IoT ?

Mi-septembre, une attaque par déni de service d'une intensité jamais enregistrée jusqu'à présent touchait OVH, avec des pics de trafic allant jusqu'à 1 Tbit/s. Si le Roubaisien a résisté à cet afflux de requêtes, l'attaque a permis de mettre le doigt sur un phénomène qui va s'amplifiant : le détournement d'objets connectés (des caméras dans le cas d'OVH), des terminaux souvent mal protégés et donc plus simples à détourner que des ordinateurs de particuliers, qui constituent habituellement le gros des troupes dans les réseaux de machines zombies servant à lancer des attaques DDoS. Qui plus est, pour les pirates, les objets de l'IoT présentent l'avantage d'être toujours connectés… dont toujours prêts à lancer une attaque.

Logique donc de voir la Commission européenne s'intéresser au sujet, même si les réflexions de Bruxelles existaient avant l'attaque contre le Français. Comme l'explique *Euractiv*, en marge d'une législation sur les télécoms, Bruxelles planche sur un corpus de règles qui devraient imposer aux constructeurs d'objets connectés de se conformer à des standards de sécurité et d'en passer par des certifications afin de garantir le respect de la vie privée des utilisateurs. « *Il ne suffit pas de regarder un composant. [Avec l'IoT], vous devez examiner le réseau, le Cloud. Vous avez besoin d'un cadre de gouvernance pour bénéficier d'une certification* », a expliqué Thibault Kleiner, le directeur de cabinet de Günther Oettinger, le commissaire à l'Economie numérique, lors d'une conférence à Bruxelles. Et d'évoquer les normes de consommation d'énergie comme source d'inspiration pour le futur label de cybersécurité.

Des failles grossières

Si le « *cadre de gouvernance* » de Bruxelles demeure très flou, Thibault Kleiner semble privilégier une initiative de l'industrie, que l'exécutif européen pourrait ensuite embrasser. En 2015, la Commission européenne a monté une plateforme visant à favoriser les usages de l'IoT ; celle-ci réunit déjà de nombreux industriels, dont Cisco, Bosch, Nokia, Philips et divers opérateurs télécoms.

L'analyse des attaques contre OVH, mais aussi contre le site du blogueur américain Brian Krebs, montre qu'il y a probablement urgence. Dans un billet de blog, la société Flashpoint explique ainsi que le malware Mirai, un de ceux servant aux pirates à bâtir leurs réseaux zombies lors des récents DDoS, s'appuie sur des failles béantes laissées par un éditeur de logiciels et fabricant d'électronique chinois, XiongMai Technologies. Ces éléments, embarqués par divers fabricants de caméras, sont construits avec un login et mot de passe (respectivement root et *xc3511*,) codés en dur dans le firmware, un accès impossible à désactiver pour peu que l'assaillant se connecte via les protocoles Telnet ou SSH. S'y ajoute une autre faille, tout aussi déconcertante de légèreté, permettant de bypasser l'authentification Web ! Selon Flashpoint, 515 000 machines embarquant les technologies de XiongMai sont touchées par ces vulnérabilités béantes. De quoi constituer un solide réseau de zombies… Signalons que certaines caméras d'un autre fabricant chinois – Dahua – sont elles aussi touchées par une faille d'authentification, tout aussi grossière.

« Impliquer la responsabilité des constructeurs »

Dans les colonnes de *Motherboard*, l'expert en sécurité Bruce Schneier se prononce clairement pour une intervention du gouvernement : « *quand le marché échoue, le recours au gouvernement est l'unique solution. Ce dernier peut imposer des règles de sécurité aux fabricants d'IoT, pour les obliger à mieux sécuriser leurs terminaux même si les consommateurs n'y prêtent pas attention. Il peut aussi impliquer la responsabilité des constructeurs, permettant à des gens comme Brian Krebs de les poursuivre. Ces mesures permettraient d'augmenter le coût de l'insécurité et donneraient à ces entreprises des incitations pour investir dans la sécurisation de leurs appareils.* »

A lire aussi :

L'Europe se mobilise pour la cybersécurité

IoT : les objets connectés, futur cauchemar pour les réseaux d'entreprise ?

crédit photo © Ugis Riba – Shutterstock