IoT : « Pirater un réseau Lora ? A quoi bon », plaide Objenious

Les objets connectés sont pointés du doigt pour leur faible sécurité. Le site du journaliste spécialisé en sécurité Brian Krebs a récemment fait les frais des faiblesses des objets connectés. Tout comme l'hébergeur OVH, contraint d'écarter des attaques DDoS massives qui visaient des sites de certains de ses clients. Des attaques lancées à partir d'objets connectés corrompus et dressés en réseau pour lancer des requêtes massives. Face à ces attaques, le cabinet Gartner invite les entreprises à mettre à jour leurs directives d'accès au réseau pour prévenir l'exploitation malveillante des objets connectés.

Mais tous les objets ne sont pas nécessairement concernés. Notamment ceux qui utilisent les réseaux à très bas débit longue portée (LPWA) comme Lora ou Sigfox. *« A raison de 50 octets par objet, il faudrait 1 milliard d'objets connectés pour mener une attaque comme celle contre OVH et Krebsonsecurity »*, estime Stéphane Allaire, dirigeant d'Objenious, la filiale Internet des objets (IoT) de Bouygues Telecom. OVH a en effet dû essuyer des charges à 1,6 Tbit/s en provenance d'objets (des caméras de surveillance et leurs enregistreurs numériques en l'occurrence) connectés à des réseaux haut débit. Une attaque issue d'un ensemble d'objets connectés sur un réseau Lora n'est *« pas impossible*, poursuit le responsable, *mais à condition de compromettre un milliard d'objets qui auraient tous la même vulnérabilité »*. Un vrai défi pour les attaquants. Enfin, il faudrait parvenir à mener l'attaque jusqu'à son terme, c'est-à-dire le site de l'entreprise visée. Or, *« la première chose qui s'écroulerait serait le réseau privé »*, confie Stéphane Allaire. Autrement dit le backbone de l'opérateur Bouygues Telecom en l'occurrence. Un mauvais calcul stratégique pour les pirates, donc.

Lora pas pour les pacemakers

La sécurité des objets en eux-mêmes n'en reste pas moins sujette à question. En septembre dernier, à la conférence Hardwear.io, le chercheur en sécurité Renaud Lifchitz démontrait que les réseaux bas débit et basse consommation (LPWA) n'affichaient pas un niveau de sécurité à toute épreuve. Il avançait qu'il était possible de déchiffrer des messages envoyés par les objets ou de récupérer le contenu de leur mémoire. Ce qu'admet Stéphane Allaire. *« Mais il faut accéder à l'objet*, ajoute-t-il. *Et pour voler quelles informations sensibles ? Des relevés de compteurs d'eau ? »*

Le dirigeant en profite pour rappeler que les réseaux LPWA s'appuient sur des fréquences libres, et donc écoutables par tout le monde, ce dont les clients ont conscience. Cependant, *« les informations qui circulent sur le réseau Lora d'Objenious sont toutes chiffrées avec une clé et le seul moyen de déchiffrer le message est d'obtenir la clé*, assure-t-il. *Le hacker affirme qu'il est possible, en récupérant l'objet et avec de gros moyens techniques, d'obtenir la clé, mais cela demande beaucoup d'efforts pour des données qui n'en valent peut être pas la peine. »*

Au besoin, ceux qui veulent à tout prix sécuriser leurs données, peuvent installer un Secure Element, un composant gravé dans la puce qui rend inaccessible la clé et donc le déchiffrement des communications même après le piratage de l'objet. Un service qui sera disponible prochainement.

« Mais aucun client ne nous l'a demandé jusqu'à aujourd'hui. » Stéphane Allaire ne prétend d'ailleurs pas que le réseau Lora réponde à tous les besoins. *« Objenious ne convient pas dans la santé*, confie-t-il. *Je ne conseillerai pas Lora comme la solution la plus adéquate pour un projet de mise à jour des données d'un pacemaker, par exemple. »*

Lora brouillable

A défaut de DDoS en bas débit, le réseau Lora pourrait-il ouvrir la porte à d'autres types d'attaques ? *« Sur Lora, je n'en vois pas, mais je fais confiance aux pirates pour en trouver*, plaisante notre interlocuteur. *Mais j'ai vu des attaques d'objets connectés, comme des ampoules Wifi, qui servent de backdoor pour pénétrer le réseau local du client. Ce qui ne peut pas arriver sur Lora car, pour espérer atteindre le réseau du client final, les attaquants sont obligés de passer sur nos passerelles et se heurteront alors à nos firewall. »* En revanche, le brouillage, volontaire ou non, de la fréquence sur laquelle opère Lora est plus plausible. La conséquence se traduirait par une perte de service partielle ou totale, mais sans toucher à l'intégrité des données. Dans ce cas, *« il n'y a pas grand-chose d'autre à faire qu'à interpeler l'auteur du brouillage »*, concède le responsable.

Autant de problématiques auxquelles n'est pas encore confronté Objenious, alors que le marché de l'IoT démarre tout juste. L'opérateur Lora revendique une trentaine de clients en production aujourd'hui (dont Primagaz, Carrefour Supply Chain ou Petit Forrestier) *« avec plein de cas d'usage différents »*. Les 4 000 antennes de l'opérateur attendues en fin d'année couvriront la quasi-totalité du territoire. Fort de son écosystème, l'entreprise dispose d'un catalogue de 50 objets connectables (une centaine en fin d'anné)e. *« Mais, l'expérience aidant, on a constaté qu'il vaut souvent mieux partir d'un objet qui n'est pas connecté mais qui rend un usage pour lui apporter une connectivité Lora plutôt que l'inverse »*, confie Stéphane Allaire. Ce qui revient à enrichir d'une connectivité un objet déjà fonctionnel. C'est probablement là que le marché de l'IoT trouvera tout son sens.

Lire également

Une faille dans OpenSSH âgée de 12 ans fragilise l'IoT
Bientôt un label européen pour la sécurité de l'IoT ?
Bouygues Telecom accélère dans l'Internet des objets avec Objenious

crédit photo iot sécurité © alice-photo – shutterstock