Apprenez à vous protéger contre le piratage de vos objets connectés du quotidien

	Apprenez à vous protéger contre le piratage de vos objets connectés du quotidien

Souhaitant mettre rapidement sur le marché leurs produits, les fabricants d'objets connectés ont eu tendance à négliger l'aspect sécurité, contribuant ainsi à la vulnérabilité de leurs utilisateurs face à de possibles attaques.

Atlantico : En septembre et octobre 2016, deux attaques DDOS ont été particulièrement marquantes : la première sur l'entreprise OVH et la deuxième sur DYN. Dans les deux cas, ces attaques ont été rendues possibles par les objets connectés. Malgré l'ampleur de ces attaques, celles-ci sont à relativiser. Dans une récente étude réalisée pour le compte de l'entreprise HSB, on note que seulement 10% des utilisateurs ont été touchés par des problèmes de piratage. Quels sont les risques du piratage des objets connectés ?

Quel peut être le préjudice porté aux particuliers et aux entreprises ?

Yvon Moysan : Une attaque DDoS ou attaque par déni de service massive vise à **rendre un serveur, un service ou une infrastructure indisponibles en surchargeant la bande passante du serveur, ou en accaparant ses ressources jusqu'à épuisement.** Lors d'une attaque DDoS, une multitude de requêtes sont envoyées simultanément et depuis de multiples endroits. L'intensité de ce « tir croisé » rend le service instable, voire indisponible. **Le risque d'être confronté à ce type d'attaque est important et surtout les tentatives sont nombreuses**. Dans le cas de la société américaine Dyn que vous évoquez, celle-ci a été victime d'une attaque de plus d'un Téra-octet par seconde, ce qui pourrait concerner environ 10 millions d'objets connectés piratés. Ce niveau d'intensité est toutefois très rare.

Le préjudice subi dépend du type d'objets connectés piratés et du caractère sensible des données des particuliers. Si la majorité des objets connectés contiennent rarement des informations aussi sensibles que celles qui sont stockées sur un ordinateur, **il en existe des sensibles comme les voitures connectées ou les fusils intelligents qui, piratés à distance, peuvent représenter un véritable danger, potentiellement mortel pour l'utilisateur.** Et **ce risque s'est d'ores et déjà avéré.** Des experts en sécurité informatique ont ainsi réussi à prendre le contrôle à distance d'une Jeep Cherokee. Ils ont pu agir sur la vitesse, freinant et accélérant à leur guise, envoyant même la voiture dans le fossé alors que pour le fusil intelligent, d'autres experts ont réussi a bloqué le déclenchement du tir.

Le risque existe également pour des objets plus communs comme les applications de smart home. Des hackers ont ainsi réussi à bloquer la température de thermostats connectés à une température polaire ou saharienne. Plus préjudiciable, des hackers ont pris le contrôle de caméras de surveillance, récupéré les vidéos enregistrées, et au final les ont diffusées sur le Web. Un baby phone a également été la cible d'un hacker terrorisant un bébé et ses parents. En prenant le contrôle de l'appareil équipé d'une caméra, d'un micro et d'un haut-parleur, celui-ci s'est mis à hurler des insanités sur le nourrisson. **Le risque peut surtout être généralisé si des hackers réussissent à prendre le contrôle des réseaux d'électricité ou de gaz sur un quartier par exemple.** Il devient en effet possible de plonger toute une zone dans le noir ou, en fonction des données récoltées sur la consommation, de savoir quelles habitations sont occupées ou pas, en vue d'éventuels cambriolages.

Cela peut ensuite être contraignant pour la société qui a fabriqué et vendu les objets piratés car cela révèle **la faiblesse du niveau de sécurité**. Dans le cas de l'attaque de la société Dyn, une partie des objets connectés étaient ceux de la société chinoise Xiongmai, qui a dû les rappeler en urgence pour leur appliquer un correctif de sécurité. Cela peut aussi être problématique pour les clients de la société victimes de l'attaque. Dans le cas de Dyn, cela a eu pour conséquence de rendre inaccessible pendant une dizaine d'heures des sites comme Twitter, Ebay, Netflix, GitHub ou encore PayPal.

On peut aussi s'interroger sur certaines pratiques des constructeurs. Le fait de mettre un mot de passe commun à tous les appareils avant une première connexion a déjà été pointé du doigt. Quels autres dysfonctionnements peut-on mettre en avant ? Face à l'augmentation du nombre d'objets connectés, comment s'adaptent précisément les constructeurs en termes de sécurité ?

Tout d'abord il est important de préciser que ce type d'attaques par déni de service n'a rien de nouveau : les cybercriminels utilisent depuis des années des armées d'ordinateurs piratés pour inonder de requêtes les sites ciblés et les rendre inaccessibles.

La nouveauté réside ici dans le nombre croissant des objets connectés qui accroit de manière exponentielle les possibilités d'attaques. Or **la puissance d'une attaque dépend essentiellement du nombre de périphériques piratés, d'où l'intérêt de passer par les objets connectés**. Il existe en effet **plusieurs milliards d'objets connectés dans le monde contre quelques centaines de millions d'ordinateurs.** Pour y faire face, il existe des solutions proposées par les hébergeurs pour protéger leurs serveurs des attaques. Ces solutions permettent, par exemple, d'analyser en temps réel et à haute vitesse tous les paquets, et si besoin d'aspirer le trafic entrant, voire de mitiger, c'est-à-dire repérer tous les paquets IP non légitimes, tout en laissant passer les paquets IP légitimes.

Du côté des constructeurs d'objets connectés, tous les thermostats, toutes les webcams ou les imprimantes ne présentent pas de faille de sécurité, mais il s'agit d'un point préoccupant car **pour la plupart des fabricants, la sécurité n'a pas été la priorité dès le départ**, **ayant souvent été donnée à la rapidité de la mise à disposition du produit sur le marché pour répondre à un nouveau besoin**. Il faudrait que des normes minimales de sécurité puissent être définies comme le cryptage des données échangées sur le réseau ou l'exigence de mot de passe sécurisé mêlant caractères spéciaux et chiffres pour l'accès à distance et l'interdiction de mots de passe comme « 123456 » particulièrement vulnérables. Dans cet esprit, la Online Trust Alliance, qui regroupe des éditeurs comme Microsoft, Symantec (Norton) et AVG, a rédigé un guide des bonnes pratiques pour minimiser les risques de piratage. Les constructeurs d'objets connectés peuvent, par ailleurs, faire évaluer leurs systèmes de cryptage par des sociétés spécialisées, pour identifier les éventuelles vulnérabilités.

Comment se prémunir du piratage d'objets connectés ? Quels sont les bons comportements à adopter ? Que faire en cas de doute ?

Du côté des particuliers, il apparait préférable de privilégier les produits de sociétés à la pointe des questions de sécurité informatique, comme Google ou Apple. Il faut également installer régulièrement **les mises à jour de sécurité et les mises à jour logicielles**, pour limiter le nombre de vulnérabilités connues qui pourraient être exploitées. Après, il faut **changer le nom et le mot de passe par défaut de chaque objet connecté, car c'est la première chose qu'un hacker tentera d'attaquer pour en prendre le contrôle.** Pour finir, il faut **limiter l'accès d'un objet connecté aux autres objets connectés dans la maison.** Par exemple, si vous avez une Smart TV, vous devrez restreindre l'accès à cette TV et autoriser seulement son accès à des ressources particulières du réseau. Par exemple, il n'est pas vraiment nécessaire que l'imprimante soit connectée à la télévision.

Réagissez à cet article

Original de l’article mis en page : Attention danger : apprenez à vous protéger contre le piratage de vos objets connectés du quotidien | Atlantico.fr