L’Internet des objets, ce piège de cristal

L’Internet des objets, ce piège de cristal

Encore une fois, l'actualité technologique nous démontre que l'Internet des objets est un problème de sécurité de masse en devenir.

Vous le savez sans doute si vous suivez mes articles, je suis un tantinet sceptique quant à la montée de l'Internet des objets, soit le mariage entre l'Internet et les objets du quotidien. Non pas que je doute des possibilités offertes par les systèmes qui émergeront de cette tendance, bien au contraire. Ce sont plutôt les problèmes de sécurité qu'ils engendreront qui me laissent quelque peu pantois.

Imaginez les grands titres : «Incapables de regarder le Canadien de Montréal à cause d'un maliciel». Je vous jure, là, les gens vont débarquer dans les rues.

Lorsqu'on prend du recul et qu'on regarde ce qui se passe, nous sommes littéralement en train de nous créer notre propre piège de cristal : c'est bien beau et reluisant à l'extérieur, mais un gros problème se cache à l'intérieur. Nous sommes en train de devenir dépendants de systèmes extrêmement poreux. Or, je ne serais pas surpris de voir que bon nombre d'objets connectés que l'on considère comme des «acquis» finissent par tomber en otage aux mains d'un Hans Gruber en puissance qui décide tout simplement de nous faire cracher le cash pour retrouver le contrôle desdits objets.
Ça semble peut-être bien théorique en ce moment, mais la journée où des voitures, des frigos, des systèmes de chauffages, ou des téléviseurs cesseront de fonctionner pour la simple et bonne raison qu'ils seront tombés entre les griffes d'un quelconque cryptorançongiciel remâché, ça risque de déranger pas mal de monde, et pire, en inquiéter encore plus. Imaginez les grands titres dans les tabloïds : «Incapables de regarder le Canadien de Montréal à cause d'un maliciel». Je vous jure, là, les gens vont débarquer dans les rues.

Die Harder

Le pire dans tout ça, c'est qu'on est véritablement devant une chronique de mort annoncée. Déjà, on a constaté que certains objets connectés pouvaient être massivement piratés par toutes sortes de moyens. Il y a quelques mois de cela, on découvrait par exemple que des ampoules et des serrures connectées ***pouvaient être ciblées et exploitées par des pirates informatiques malintentionnés****. On imagine déjà le potentiel de ce genre de vulnérabilités pour la sécurité résidentielle. Pourtant, on en est qu'aux débuts en ce qui concerne les problèmes dans les systèmes de sécurité.*

(Photo : ***Frédéric Bisson****)*

Tout récemment, on a d'ailleurs vécu le comble de l'ironie dans les systèmes de sécurité alors que pas moins de 25 000 caméras de surveillance ont fait partie ***d'un réseau de botnets lançant des attaques par déni de services****. Grosso modo, des pirates informatiques ont été en mesure de pirater des caméras de surveillance mal sécurisées, de les fédérer dans un réseau sous un serveur de commandement et de contrôle et de les réutiliser pour commettre des attaques informatiques ultérieures. C'est-y pas beau ça!?*

Pourtant, on avait déjà eu des signes avant-coureurs de ce genre d'attaques. Des réseaux de botnetsconstruits avec des caméras de surveillance avaient déjà ***été découverts dans des analyses précédentes****. Des analyses qui démontraient par ailleurs que ces objets connectés étaient passablement poreux.*
Et on est loin d'être sortis du bois, je vous en passe un papier. Non seulement il existe ***des moteurs de recherche permettant de trouver les objets connectés*** *présents sur Internet, mais en plus, on a des petits génies informatiques qui se mettent à les* ***géolocaliser en utilisant des drones****. Donc, si vous aviez espoir que ça ralentirait quelque peu, détrompez-vous.*

Pourtant, je ne suis pas le seul qui a des problèmes de sommeil par rapport à cette situation. En 2014, Europol prédisait ***qu'un meurtre mené par Internet allait probablement se produire dans les prochains mois****. Bon, moi je n'irais pas jusqu'à faire une prédiction temporelle, mais c'est clair que, tôt ou tard, un truc du genre va finir par arriver. Je ne suis pas certain que ce sera un événement intentionnel, mais considérant la vitesse à laquelle on intègre des objets connectés dans le réseau de la santé, ce n'est qu'une question de temps avant que quelqu'un meurt suite à un incident informatique.*

Marche ou crève

Bon, j'ai beau couiner et geindre, c'est bien dommage, mais on ne changera pas pour autant les avancées technologiques. Le néo-luddisme ne sert strictement à rien dans ce cas; il faudra à terme que l'industrie atteigne un niveau de maturité suffisant pour construire les objets connectés avec une architecture centrée sur la sécurité. En attendant, on est dû pour quelques coups fumants de piratage et de prises d'otages numériques.
En fait, la vraie question que l'on doit se poser est celle du «retour sur investissement». Dans le cas du secteur de la santé par exemple. Oui, c'est clair que des gens finiront par mourir dus à des problèmes liés à l'informatique. Cependant, il faut aussi considérer l'autre côté de la médaille, c'est-à-dire combien de personnes ont été sauvées par ces mêmes systèmes informatiques.
Il en va de même avec les gestes que posent John McClane dans la série Die Hard. Oui, il finit par causer beaucoup de dommages et par tuer beaucoup de monde au cours de ses aventures, mais il sauve également la vie de centaines de victimes innocentes.

Yippee Ki-Yay Mother$&@%!*
Article original de Benoît Gagnon

Réagissez à cet article

Original de l'article mis en page : L'Internet des objets, ce piège de cristal | Branchez-vous