PRES@JE.COM
Droit, Economie, Justice
Rédaction : Jacques Barraux et Albert Merlin
OCTOBRE 2014 - N°24

L'Internet des objets : le nouveau cheval de Troie.

par Jean-Luc Girot, *président de Pereire Consulting.*

Les prophéties de George Orwell se réalisent. A cette nuance près que ce n'est pas un ministre de la Vérité qui nous espionne. Les internautes ignorent les yeux et les oreilles qui surveillent leur mobile ou leur PC explique Jean-Luc Girot. On ira plus loin avec les objets connectés.

En 1984, Winston Smith est employé du parti extérieur au ministère de la Vérité, c'est du moins le personnage que George Orwell met en scène en 1949 dans son roman dystopique intitulé « 1984 ». A cette époque, la police de la pensée est un organe de répression qui place dans chaque foyer un « Télécran ». Il s'agit d'un téléviseur chargé de diffuser des messages du Parti, doublé d'un système de vidéosurveillance capable d'espionner l'intimité des foyers.

En 2014, il n'existe pas plus de ministère de la Vérité que de police de la pensée, fort heureusement, mais les « Télécrans » sont bien là. Non point qu'ils fussent imposés par un quelconque gouvernement totalitaire, non, bien pire que cela, ils sont installés de plein gré par les citoyens eux-mêmes. Le « Télécran » c'est le micro-ordinateur, ou la tablette équipée de sa webcam. On l'installe partout, la connecte à Internet, sans maîtriser le moins du monde ses fonctions cachées et ouvre son univers à tous les hackers de la planète, avides de collecter des informations pour en tirer quelque funeste parti.

La technologie Internet n'est réellement maîtrisée que par une minorité de spécialistes. Qui d'entre nous peut certifier qu'il n'est pas observé et que son accès internet n'est pas piraté à son insu ?

Une mauvaise nouvelle arrivant rarement seule, que penser des objets connectés qui pénètrent insidieusement dans nos foyers ? A peine digérés le web 2.0 et ses réseaux sociaux que voici poindre à l'horizon le web 3.0 également nommé : l'Internet des objets. Le premier se nomme « Nabaztag », il s'agit d'un sympathique lapin né en 2005. Connecté à Internet, il avait pour vocation principale de lire à haute voix les messages reçus sur une boîte email et de changer de couleur en fonction de la météo. Aujourd'hui, la tendance s'accélère et les objets connectés se multiplient pour notre plaisir et notre confort : vélos qui mesurent l'effort, valises qui se retrouvent toutes seules, clés qui ne se perdent plus, plantes qui s'arrosent quand elles ont soif, etc. La liste est déjà longue et s'allonge quotidiennement.

Quels sont les objets connectés et comment fonctionnent-ils ?

Les objets connectés ne constituent pas une catégorie à part. Tous les objets du quotidien sont candidats à la connexion dès qu'ils sont équipés d'un dispositif leur permettant de communiquer leur activité à leur écosystème, via un réseau sans fil. Prenons par exemple les lampes d'ambiance connectées. Elles sont pilotables par un smartphone ou par l'ordinateur familial. Elles changent de couleur et modifient l'ambiance lumineuse de la maison à l'envi. Tout est simple, elles se connectent par le réseau wi-fi domestique et se reconnaissent entre-elles automatiquement. C'est magique...

Mais voilà qu'au cours de l'été 2014, un groupe anti-piratage a réussi à intercepter les messages véhiculés entre les lampes du système – dans lequel figuraient les clés d'accès au réseau wi-fi –, mettant immédiatement à mal ce dernier et donnant accès à l'ensemble du réseau concerné. Informé, le fournisseur de lampes a réagi et a modifié son protocole d'accès, mais la preuve est faite que chaque objet connecté présentera toujours une faille. Ainsi, la multiplication de ces derniers constitue une réelle menace pour la sécurité de nos réseaux, de nos données et par extension de la nôtre.

Cette malheureuse expérience se renouvellera inéluctablement sachant que la sécurité informatique « absolue » n'existe pas. Tout est question de course à la complexité et à la puissance qui ne finit jamais. Il est probable que les futurs objets connectés afficheront une norme de relative protection aux attaques des hackers, mais ils seront toujours vulnérables d'une manière ou d'une autre.

Inutile de le nier, les objets connectés constituent une nouvelle faiblesse des réseaux et des systèmes d'information qui multiplient et diversifient les méthodes d'intrusion, comme d'innombrables portes

difficiles à sécuriser, voire même à identifier. Sera-t-il toujours possible d'établir la liste exhaustive des objets connectés en sa possession ? Des intrus ne pourront-ils pas se glisser dans nos systèmes ? Comment pourrons-nous garantir leur intégrité ? Il est encore trop tôt pour répondre à ces questions.

Alors, faut-il se résigner et lutter de toutes nos forces contre le développement de ces indésirables ? C'est à chacun d'entre nous de répondre à cette question, d'estimer son propre risque et de tenter d'évaluer son exposition au piratage potentiel, mais en connaissance de cause !

Télécharger le PDF de l'article

<< Retour au sommaire

PRES@ JE.COM

Une publication de l'Institut PRESAJE
(Prospective, Recherche et Etudes Sociétales Appliquées à la Justice et à l'Economie)
Siège social : 2 avenue Hoche 75008 Paris - Courrier : 30 rue Claude Lorrain 75016 Paris
Tél. 01 46 51 12 21 - E-mail : contact@presaje.com - www.presaje.com
Directeur de la publication : Michel Rouger

Pour ne plus recevoir d'e-mails de la part de Presaje, cliquez ici >> CONSULTER LES PRECEDENTS NUMEROS