Des fabricants d’objets connectés poursuivis en raison de failles de sécurité

Des fabricants d’objets connectés poursuivis en raison de failles de sécurité

La Federal Trade commission (FTC) américaine poursuit un troisième fabricant, l'accusant de mettre en danger la sécurité des consommateurs et la confidentialité de leurs données, en raison de la sécurité inadéquate de son routeur et de ses webcams. Derrière cette troisième plainte, c'est tout un plan d'action qui se dévoile en vue de contraindre les fabricants à augmenter le niveau de conception des objets connectés, même ceux d'entrée de gamme.

Et de trois ! La plainte déposée en janvier 2017 contre D-Link fait partie du plan de campagne de la FTC visant à renforcer la confidentialité et la sécurité des consommateurs par rapport à ce que l'on appelle l'Internet des objets (IoT). La FTC avait déjà dégainé deux fois, contre ASUS (un fabricant de matériel informatique) et TRENDnet (un distributeur de caméras vidéo).

IoT ?

Internet se transforme progressivement en un réseau étendu, appelé « Internet des objets », reliant tous les objets devenus connectables. Cette évolution soulève de nombreuses questions concernant la croissance économique et les mutations sociales, mais aussi les libertés individuelles et la souveraineté nationale, auxquelles les décideurs publics devront au plus tôt répondre. (http://www.strategie.gouv.fr).
Selon certaines études, c'est pas moins de 80 milliards d'objets connectés qui interagiront d'ici 2020. De la montre intelligente au téléphone, en passant par le frigo connecté, la webcam, le système d'alarme, la domotique, les outils de Smartcities (parcmètres, etc.), … la liste est quasiment infinie.
À côté des enjeux sociétaux, il y en a un autre dont on parle de plus en plus souvent : la sécurité.

La sécurité, enjeu technique mais aussi juridique

Les objets connectés ont, pour certains, mauvaise réputation. Surtout lorsqu'il s'agit objets connectés ayant une petite valeur économique. On songe par exemple aux webcams connectées à l'Internet. On peut en acheter pour quelques dizaines d'euros. Le problème vient du fait qu'étant connectés à l'Internet, ces objets représentent un point de faiblesse s'ils ne sont pas bien conçus et protégés. Une personne malintentionnée peut utiliser cet appareil connecté pour pénétrer le réseau, et ensuite s'y balader.
Exemples : si le système d'alarme connecté à l'Internet est mal protégé au niveau du routeur, on pourrait le désactiver à distance et entrer dans la maison. Si la webcam est mal protégée, on pourrait observer à distance une personne, voire enregistrer ses conversations, et la faire chanter ensuite.
La Federal Trade Commission a déposé une plainte contre le fabricant de matériel de réseau informatique Taiwanais D-Link Corporation et sa filiale américaine, alléguant que les mesures de sécurité inadéquates prises par la société ont laissé ses routeurs sans fil et caméras Internet vulnérables aux attaques de pirates, mettant en danger la sécurité et la vie privée des consommateurs américains.
Dans une plainte déposée dans le district nord de la Californie, la FTC a accusé D-Link de ne pas prendre de mesures raisonnables pour sécuriser ses routeurs et ses caméras (de surveillance) connectées, créant un risque important pouvant aller jusqu'à l'interception des flux audio et vidéo. En clair : on vous observe en vidéo ou on vous écoute, sans que vous le sachiez !
Pour la FTC, *« les pirates informatiques ciblent de plus en plus les routeurs et les caméras IP – et les conséquences pour les consommateurs peuvent inclure non seulement un problème de défectuosité du matériel, mais aussi un enjeu en termes de sécurité de l'individu et de sa vie privée. Lorsque les fabricants disent aux consommateurs que leur équipement est sécurisé, il est essentiel qu'ils prennent les mesures nécessaires pour s'assurer que ce soit vrai ».*

La sécurité est-elle défaillante ?

La FTC relève notamment :
• Défaut de sécurité lié aux identifiants de connexion intégrés en usine. Si tous les appareils d'un même modèle sortent de l'usine avec un paramétrage par défaut comprenant une identification et un mot de passe identiques, le risque est important que ces réglages d'usine ne soient pas modifiés par l'utilisateur, créant une voie d'entrée royale pour les pirates ;
• Sécurité insuffisante par rapport aux attaques par injection de commande. Ces attaques permettent d'utiliser une page d'erreur pour poser une série de questions de type True/False afin de prendre le contrôle total de la base de données ou d'exécuter des commandes sur un système. On en a beaucoup parlé avec les consoles de jeu en 2016.
• Mauvaise gestion d'un code d'accès privé utilisé pour se connecter au logiciel D-Link, ouvert sur un site public pendant six mois ;
• Absence de sécurisation des informations d'identification des utilisateurs pour l'application mobile (texte clair et lisible sur les appareils mobiles) alors qu'il existe des logiciels disponibles pour sécuriser ces informations.
Selon la plainte, les pirates pourraient exploiter ces vulnérabilités en utilisant plusieurs méthodes relativement simples.
Par exemple, en utilisant un routeur compromis, un pirate pourrait obtenir les déclarations de revenus des consommateurs ou d'autres fichiers stockés sur le périphérique de stockage attaché du routeur. Ils pourraient rediriger un consommateur vers un site Web frauduleux ou utiliser le routeur pour attaquer d'autres périphériques sur le réseau local, tels que des ordinateurs, des smartphones, des caméras IP ou d'autres appareils connectés.
Autre exemple : la FTC allègue qu'en utilisant une caméra compromise, un pirate pourrait surveiller le lieu où se trouve le consommateur afin de les cibler en cas de vol ou d'autres crimes, ou de regarder et d'enregistrer leurs activités personnelles et leurs conversations.

Original de l'article mis en page : Internet des objets : des fabricants poursuivis en raison des failles de sécurité des objets connectés – Droit & Technologies

---

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Internet des objets : des fabricants poursuivis en raison des failles de sécurité des objets connectés – Droit & Technologies