Les objets connectés, portes d'entrée grandes ouvertes aux hackers

Avec la démocratisation des objets connectés viennent les immanquables failles de sécurité, trop peu connues du grand public mais facilement exploitables par les connaisseurs.

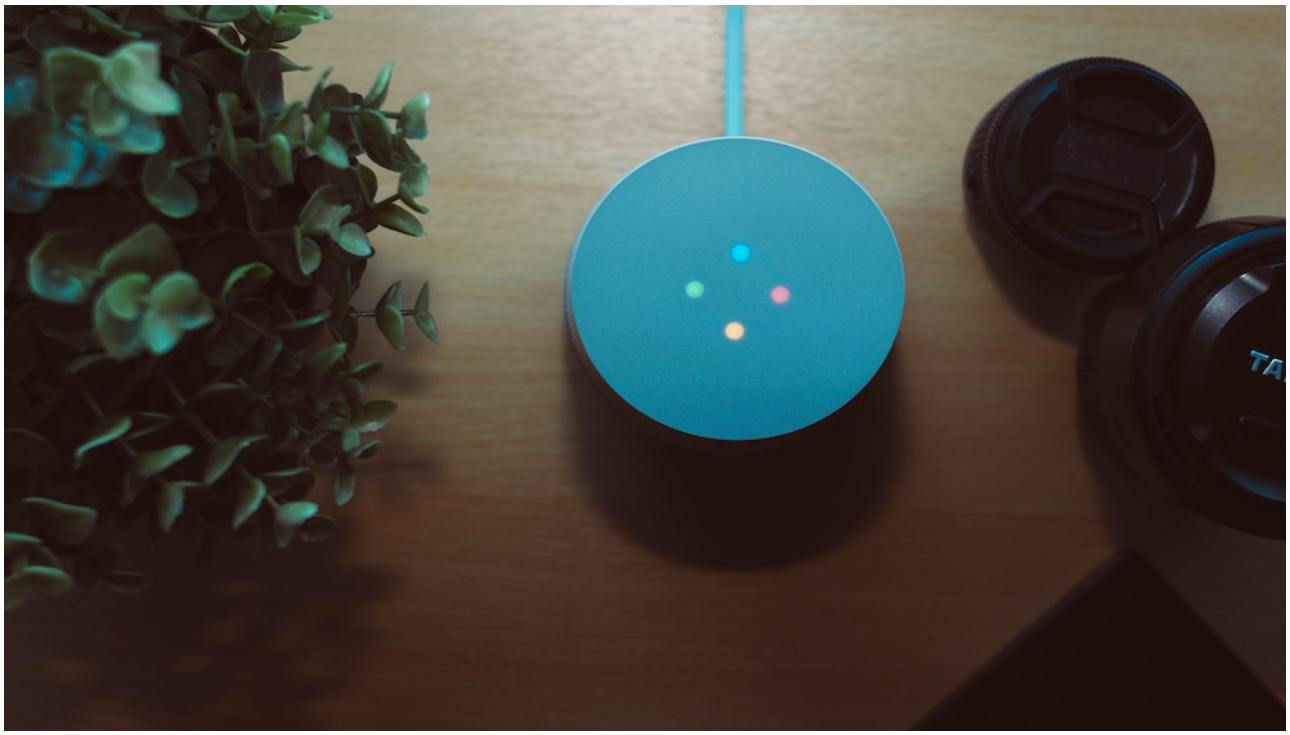
Temps de lecture : minute

28 janvier 2020

Une montre connectée, un nounours qui fait de la musique pour endormir les enfants, un réfrigérateur... Inoffensifs en apparence, ces objets peuvent être détournés à des fins malveillantes mais aussi devenir des témoins de crimes, utiles auxiliaires pour les enquêteurs. Lors du Forum international de la cybersécurité (FIC) qui se tient de mardi à jeudi à Lille, la gendarmerie - à l'origine de la création du forum en 2007 - présentera son Plateau d'investigation sur les objets connectés (PIOC), qui a tout juste un an.

Avec l'engouement du public pour les objets connectés à internet, avec moins de sécurité qu'un ordinateur, est apparue une nouvelle forme de criminalité: cela va du ransomware à la fabrication de cryptomonnaie en passant par les cambriolages sans effraction, les escroqueries ou le harcèlement. "*Ces objets, qui font partie de notre quotidien, ont peu de mises à jour et vont créer des vulnérabilités. Un malfaiteur pourra capter vos données par son intermédiaire*", résume la lieutenant-colonel Fabienne Lopez, cheffe du Centre de lutte contre les criminalités numériques (C3N) basé à Pontoise (Val d'Oise). La domotique peut s'avérer désastreuse si des malfaiteurs parviennent à la détourner. Des cambriolages sans effraction deviennent ainsi possibles, comme le sont

depuis longtemps les vols de voitures par la copie de la fréquence de la clé de contact.



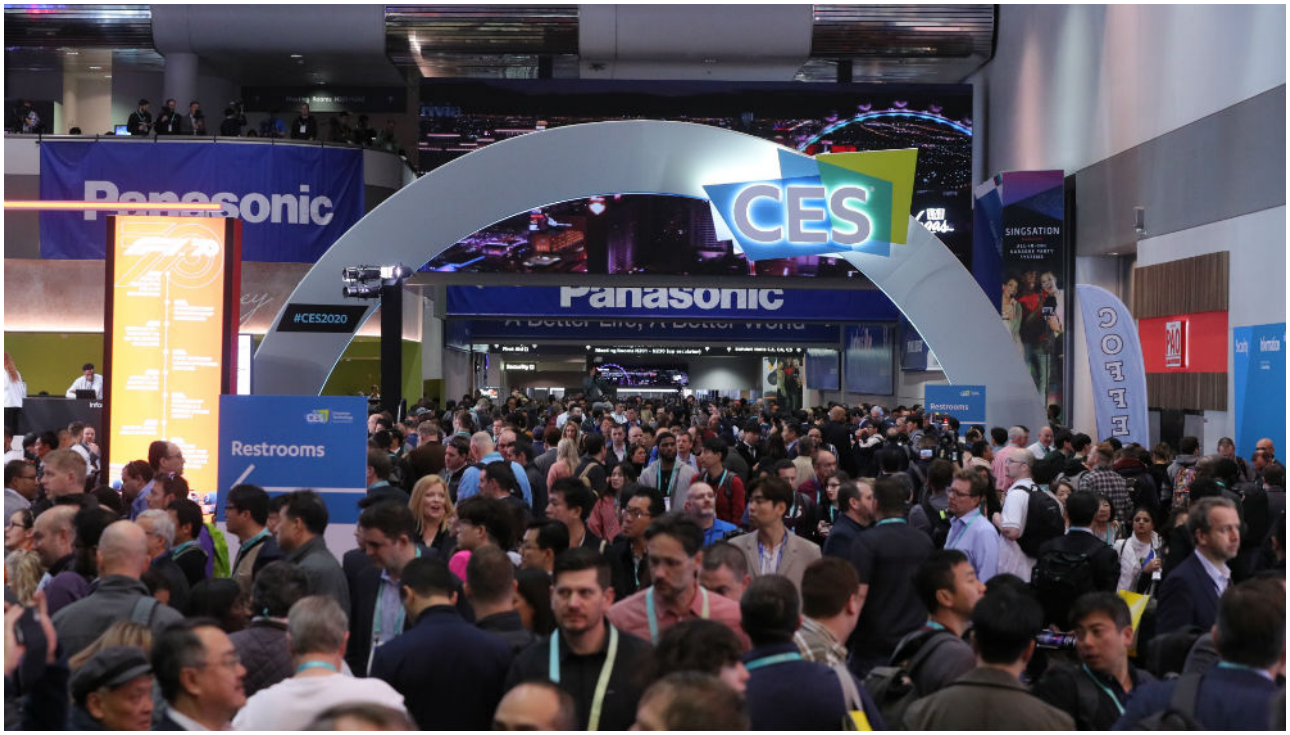
À lire aussi
Objets connectés : "Nous n'en sommes qu'au début de la vague"

En 2019, plus de 82.000 infractions à caractère cyber ont été constatées par les unités de gendarmerie, soit une progression de plus de 20% par rapport à 2018. Les escroqueries représentent plus de 70% de ce contentieux. La gendarmerie a été saisie d'environ 250 faits de ransomware. Un chiffre relativement stable mais qui reste bien en-deçà de la réalité. "*Trop de particuliers et d'entreprises préfèrent payer les rançons dans l'espoir de récupérer leurs données. Mais ils paient, récupèrent leurs données et se font attaquer de nouveau*", relève Fabienne Lopez. Des entreprises "*hésitent à déposer plainte par peur que ce signe de fragilité soit divulgué*", note-t-elle aussi.

Fraude, pédopornographie et espionnage

Mais depuis peu, les enquêteurs ont ajouté à leurs investigations l'examen des objets connectés présents sur une scène de crime car ils peuvent utilement orienter leur enquête. Il en est allé ainsi d'un homme venu expliquer aux gendarmes combien l'incendie de sa maison l'avait traumatisé. Soupçonnant un incendie volontaire, les enquêteurs ont examiné sa montre connectée qui a révélé que son rythme cardiaque n'avait pas varié au moment de la découverte de l'incendie. "*En fait, il n'était pas du tout angoissé. Ce n'était pas une preuve, mais cela a fourni un élément d'enquête*", a commenté la cheffe de C3N. Un père en instance de divorce avait quant à lui trouvé le moyen de détourner l'usage d'un nounours connecté - il diffusait de la musique dès que l'enfant pleurait - pour espionner son épouse. L'examen du jouet a permis de le démasquer.

Dans ce domaine, l'imagination n'a pas de limite, souligne Pierrick B., le capitaine commandant du PIOC. Un pédophile s'était servi d'un répéteur Wifi (amplificateur de signal) pour entrer dans le réseau wifi de son voisin. Cela lui permettait de consulter des images pédopornographique sur le net en faisant porter les soupçons sur son voisin. Un autre stockait ce type d'images dans un déodorant à bille. En retraçant le flux informatique, les enquêteurs sont parvenus jusqu'au système de stockage inséré dans le déodorant, qui fonctionnait tout à fait normalement.



À lire aussi
A Las Vegas, les startups françaises de l'IoT bonnes élèves de la protection des données

Phénomène relativement courant : la fabrication de cryptomonnaie par des malfaiteurs qui pénètrent dans les objets connectés. "*On ne s'en aperçoit pas forcément. L'objet a des ralentissements mais c'est tout*", souligne Pierrick B. Parmi les faits d'armes du C3N figure le démantèlement du virus informatique international Retadup. Le botnet utilisé (réseau d'ordinateurs) avait infesté 1,3 million d'ordinateurs dans le monde. "*Il a fallu trouver un moyen pour neutraliser le virus sans entrer dans les ordinateurs concernés*", raconte Fabienne Lopez, soulignant qu'aucune trace de la manoeuvre n'avait été laissée dans les ordinateurs.

Maddyness avec AFP

Article écrit par Maddyness avec AFP