CONTRE-ENQUÊTE

Les objets nouvelle cible des

Plus de cinq milliards d'appareils sont reliés à Internet. Mais à force d'en négliger la sécurité, les fabricants déroulent un boulevard aux pirates.

C'était une belle soirée d'été. Marc Gilbert venait tout juste de débarrasser la table, après avoir savouré un bon barbecue en famille, lorsqu'il entendit une voix grave venant de la chambre d'Allyson, sa petite fille de deux ans. Paniqué, le jeune père de famille texan se précipite alors à l'étage où il découvre avec horreur qu'une voix sordide s'échappe de la babycam connectée au réseau Wifi de la maison. "Réveille-toi", brame un sinistre individu à travers le haut-parleur de l'appareil, installé à côté du lit du bébé. Affolé, Marc Gilbert se fait ensuite injurier, avant de réaliser que cette voix d'outre-tombe n'est pas celle d'un revenant. C'est un pirate qui a pris le contrôle du visiophone pour proférer ses insanités ! Quelques mois avant l'incident, des chercheurs américains avaient pourtant alerté sur la vulnérabilité de ces appareils, de marque Foscam. Mais leur rapport était quasiment passé inaperçu, pour le plus grand bonheur des flibustiers du Net...

L'envers du confort. Il va falloir s'y faire. Après les PC et, plus récemment, les smartphones, les hackers ont trouvé leur nouvelle cible, l'Internet des objets. Dans cet univers connecté, les ustensiles de notre quotidien sont dotés de capacités de communication et d'analyse inédites pour nous offrir davantage de souplesse et de performances. Souvent pilotables à distance, depuis un smartphone ou une tablette, ils nous promettent, entre autres, de faire des économies d'énergie (thermostat), de veiller sur notre maison en notre absence (caméra de vidéosurveillance), de mesurer notre activité physique (montre, bracelet), et tout un tas de services conçus pour nous simplifier la vie.

Le hic, c'est qu'en reliant les équipements les plus banals de notre environnement au réseau, les fabricants ouvrent en même temps un boulevard aux hackers. "Ces objets connectés sont encore plus faciles à pirater que des PC, des ordinateurs portables ou encore des tablettes", notent les techniciens de la société de cybersécurité Proofpoint dans un rapport publié l'année dernière. D'un point de vue technique, ces accessoires high-tech fonctionnent comme un petit ordinateur. Ils sont dotés d'une mémoire, d'un processeur, traitent des données... et pourtant, à ce jour, aucun d'eux n'embarque le moindre antivirus, leur protection restant le cadet des soucis des fabricants. "Leur priorité, c'est de lancer de

Pacemaker tueur Un hacker a pu déclencher des décharges électriques sur un stimulateur cardiaque. De quoi provoquer un infarctus.

ISTOCKPHOTO - DR

Frigo spammeur Voilà un peu plus d'un an, un frigo similaire a été transformé en serveur de messagerie pour envoyer des spams.

connectés, hackers

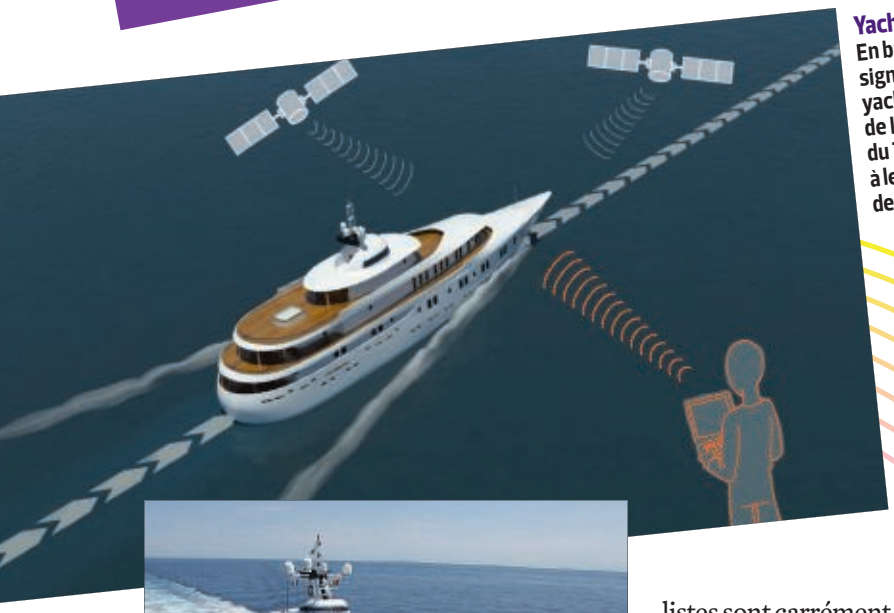
Black-out domotique Un chercheur en sécurité a trouvé le moyen de désactiver ces ampoules connectées pour plonger la maison dans l'obscurité.

nouveaux modèles au plus vite dans le but de prendre de l'avance sur leurs concurrents, explique Laurent Heslault, expert en menaces informatiques chez le géant de la cybersécurité Symantec. Intégrer de la sécurité accroît les coûts, donc le prix de vente, et retarde la commercialisation." À quoi bon s'embarrasser ? D'autant qu'au moment de l'achat, le consommateur s'intéresse essentiellement au design et aux fonctionnalités de l'engin plutôt qu'à son blindage numérique...

Mot de passe oublié. Du coup, les failles pullulent. Après avoir décortiqué dix de ces produits connectés, les petits génies du département de sécurité informatique de HP en ont répertorié 25 ! En cause ? Leur système d'exploitation, aussi facile à pénétrer qu'une passoire, mais aussi les données personnelles transmises en clair, sans aucun chiffrement... Ou encore la négligence des utilisateurs, qui prennent rarement le temps de verrouiller l'accès à l'aide d'un mot de passe. Résultat, alors que l'ère des outils connectés n'en est qu'à ses tout débuts, les pirates s'en donnent déjà à cœur joie. L'année dernière, des bidouilleurs avaient pénétré un e-réfrigérateur pour le transformer en plateforme de spamming. Les cybermalfrats avaient ensuite utilisé la messagerie intégrée dans ce frigo high-tech pour envoyer des centaines de milliers d'e-mails indésirables. Inoffensif ? Dans ce cas précis, oui. Mais il y a plus embêtant. Souvent, les flibustiers numériques entrent par cette porte dérobée du réseau pour accéder ensuite à votre ordinateur, votre mobile ou votre tablette, par exemple dans le but d'y introduire un programme malveillant. Ils peuvent également exploiter les informations mémorisées dans le dispositif pour préparer un méfait, comme un cambriolage. En Allemagne, des hackers ont ainsi démontré qu'il était possible d'intercepter des données transmises par un compteur d'électricité "intelligent", assez semblable, sur le principe, à celui qu'ERDF compte imposer en France dans tous les foyers d'ici à 2020. En accédant à ces informations, ces gros curieux ont pu détecter le nombre d'ordinateurs connectés au domicile, mais aussi quelle chaîne de télévision les habitants étaient en train de regarder.

Compteur bavard. Jusque-là, toujours rien de très grave. Sauf que l'analyse des données de consommation d'énergie, émises toutes les dix minutes, est aussi très pratique pour identifier les heures de lever et de coucher, ainsi que les périodes d'absence des habitants du domicile. Du pain bénit pour tous les disciples d'Arsène Lupin ! "Les informations de consommation d'énergie transmises par les compteurs sont extrêmement détaillées et en disent long sur les occupants d'un foyer", confirme la Cnil, l'autorité indépendante qui veille sur notre vie privée. Les distributeurs devront donc apporter des garanties sérieuses

Photos volées Les pirates savent intercepter le flux Wifi de certains reflex numériques pour dérober des photos ou déclencher des clichés.



Yacht déboussolé
En brouillant les signaux GPS d'un yacht, des étudiants de l'Université du Texas ont réussi à le détourner de sa trajectoire.

UNIVERSITE DU TEXAS - AFP - DR

sur la sécurisation de ces données. En France, ERDF affirme que son compteur Linky n'exploite pas le même protocole de communication que son cousin allemand. Et pour garantir que son compteur intelligent est inviolable, l'entreprise assure que la transmission des données est cryptée.

Un annuaire des objets à risque. Ces précautions font hélas figure d'exception. Il suffit d'aller faire un tour sur Shodan pour s'en persuader. Conçu par John Matherly, un informaticien américain, ce moteur de recherche répertorie et localise les équipements exposés au risque de piratage. On y trouve plusieurs centaines de milliers d'appareils, dont des caméras, des téléviseurs, mais aussi des climatiseurs, des chambres froides, le tableau de bord d'une centrale électrique, le logiciel de gestion d'un barrage électrique, un système de contrôle d'aiguillage de trains, le tout, bien évidemment, connecté à Internet... et dénué de toute protection. Dès lors, nul besoin d'être un pro en informatique pour pénétrer ces installations, à partir des adresses IP affichées sur Shodan. En Norvège, deux journalistes sont carrément parvenus à faire chuter la température d'un immeuble après avoir piraté un thermostat. En France, Gurvan Kristanadjaja, un journaliste du site d'informations Rue89, s'est aussi servi de Shodan pour infiltrer plusieurs systèmes de surveillance en région parisienne. "En quelques heures, j'ai localisé des dizaines de caméras, confie-t-il. Les modèles anciens de webcams fonctionnant sous Windows XP, on arrivait à les pirater pratiquement à tous les coups. Les modèles plus récents, une fois sur dix en moyenne. C'était incroyable : une fois qu'on avait pris le contrôle de la caméra, on pouvait la diriger comme on le souhaitait." L'une d'entre elles, située dans une pharmacie, filmait les clients à la caisse en train de taper leur code de carte bancaire...

Pas de quoi rassurer les fonctionnaires du très sérieux Europol, l'agence européenne de police criminelle. L'institution craint que ces nombreuses failles de sécurité finissent par entraîner une recrudescence du nombre de chantages et de kidnappings. Elle redoute notamment que les criminels détournent ces dispositifs de leurs fonctions premières pour les retourner contre leur propriétaire.

En pratique, un ravisseur pourrait hacker votre bracelet connecté pour vous localiser précisément grâce à sa puce GPS pendant que vous faites votre jogging. En bloquant la fermeture des portes à distance, il pourrait aussi vous séquestrer dans votre voiture en attendant que vous payiez une rançon. Ou même, si vous êtes diabétique, vous tuer en désactivant à distance votre pompe à insuline connectée. Un assassinat numérique ? On se croirait dans Homeland ! Dans cette série américaine, les scénaristes avaient imaginé que des terroristes avaient eu la peau du vice-président des États-Unis en sabotant son pacemaker

Voiture détournée
Depuis un smartphone, un pirate peut prendre le contrôle d'une Google Car.

connecté. Ce n'est plus de la science-fiction. Déjà en 2007, le cardiologue de Dick Cheney, alors vice-président de George W. Bush, n'avait-il pas ordonné à son illustre patient de désactiver les fonctions sans fil de son défibrillateur ? Si, pour l'heure, aucun

meurtre de ce genre n'a été déploré, les chercheurs estiment tout à fait plausible qu'un pirate implante un virus dans un accessoire médical et ralentisse son fonctionnement… avant d'asséner le coup de grâce. Barnaby Jack, un Néo-Zélandais qui s'était distingué en vidant des distributeurs de billets, en a fait publiquement la démonstration en 2012. Depuis son ordinateur, il a pris le contrôle d'un stimulateur cardiaque et envoyé des décharges de 830 volts !

Mais aujourd'hui, ce sont surtout les voitures qui intéressent les hackers. En février dernier, un responsable de la Darpa, l'agence R&D de l'armée américaine, a fait sensation lors d'une émission de télévision en pénétrant le système de communication d'urgence d'un véhicule. Alors même que le conducteur se trouvait à l'intérieur, l'expert était en mesure d'appuyer sur l'accélérateur et de désactiver les freins. Cette opération pourrait être à l'origine du décès de Michael Hastings, un journaliste retrouvé mort au volant de sa Mercedes il y a deux ans. Certains spécialistes l'affirment, c'est le piratage à distance de sa berline qui expliquerait la disparition de cet homme, qui avait reçu des menaces de mort suite à la révélation de divers scandales sur les interventions américaines en Afghanistan et en Irak. Info ou intox ? Les constructeurs automobiles tentent d'apaiser les craintes, mais même les plus réputés d'entre eux se trouvent pris en défaut. En atteste l'étude sortie en février par l'association d'automobilistes allemande ADAC, qui a mis le doigt sur une faille majeure dans la plateforme ConnectedDrive de BMW. Ce système sert notamment à géolocaliser un véhicule et à le déverrouiller à distance. Le fabricant bavarois, d'ordinaire réputé pour sa fiabilité, a fini par reconnaître que le chiffrement des données était insuffisant. Il a lancé en urgence un correctif (patch) de son système pour les 2,2 millions de véhicules concernés.

L'industrie prend la menace au sérieux : les marques jouent leur réputation

Ne cédons pas pour autant à la panique. "Les constructeurs automobiles et les marques d'électroménager prennent ce sujet très au sérieux", assure Laurent Heslault. "La moindre révélation d'une vulnérabilité avérée peut nous faire perdre la confiance du marché", confirme Romain Paoli, chef de produit chez Netatmo, un fabricant français qui commercialise notamment un thermostat et une caméra connectés. "On ne va pas prendre ce risque à la légère…" Pour l'instant, la grande majorité des cas avérés de hacking sont des simulations de chercheurs et d'informaticiens qui souhaitent sensibiliser le grand public et l'industrie. Les "vrais" pirates ne s'intéressent que modérément à ces nouveaux instruments, en raison notamment de leur nombre encore limité. "Aucun de ces produits n'est suffisamment déployé pour présenter un intérêt d'attaque massive", résume Loïc Guezo, expert en sécurité chez Trend Micro. On ne perd rien pour attendre. D'ici à la fin de la décennie, estime le cabinet IDC, le nombre d'objets connectés de la planète devrait allégrement dépasser les 200 milliards. ■

THOMAS LESTAVEL

Caméras aveuglées
L'an dernier, à Nice, dans l'émission Envoyé Spécial, un hacker a désactivé des caméras Wifi de surveillance. Utile, pour préparer son braquage incognito.

Game of trône
Un expert en cybersécurité a hacké ces toilettes japonaises Lixil Satis. Et s'est amusé à actionner les jets d'eau et la fermeture du couvercle.

Pub aguicheuse
À Moscou, un pirate malicieux a diffusé une vidéo porno sur un panneau géant en bordure de périph.