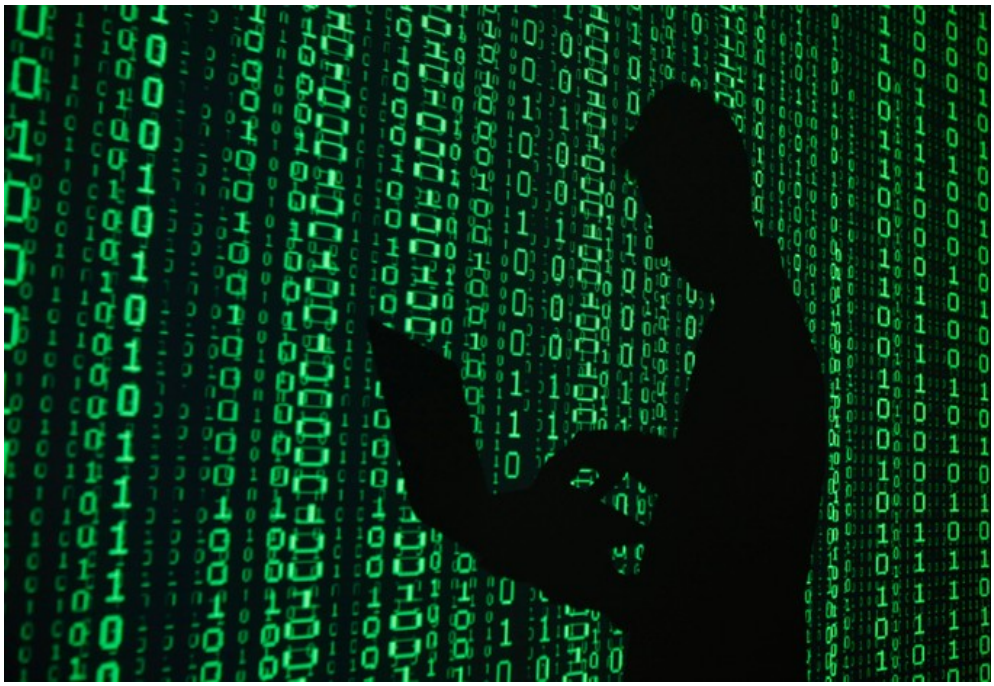
Et si le objets connectés faisaient tomber Internet ?



Et si le objets connectés faisaient tomber Internet ?

Les milliards de caméras, thermostats intelligents et autres téléviseurs reliés au réseau sont recrutés par les hackers pour former des « armées zombies » d'une puissance inégalée. De quoi couper l'accès Internet à des pays entiers.

Plus de 8,4 milliards d'objets connectés seront utilisés partout dans le monde en 2017, d'après le cabinet d'étude Gartner. Une véritable déferlante : caméras, thermostats intelligents, téléviseurs, ou même peluches et machines à café.
Des objets bien pratiques mais qui souffrent d'une défaillance majeure : ce sont de véritables passoires en termes de sécurité informatique. Un **«cauchemar»** se prépare, alerte le directeur technique de la société Avast, Ondrej Vlcek. **«De simples babyphones connectés ont été piratés pour espionner chez les gens ou pour faire peur à l'enfant en pleine nuit»**, rappelle de son côté la Cnil (Commission nationale de l'informatique et des libertés). Il est aussi possible de prendre le contrôle d'un téléviseur et de bloquer son accès en échange d'une rançon.

Des millions d'attaques simultanées

Mais plus que d'effrayer les petits enfants, les pirates poursuivent un objectif bien plus ambitieux : recruter un maximum d'objets connectés pour les transformer en réseau de zombies, les « botnets ».

Les objets connectés investissent notre quotidien. Comme Memoo, cette station digitale connectée au smartphone des parents permet de converser avec les enfants. (Photo : Deborah Lesage Aurent Gehant)

Le plus connu des logiciels malveillants, Mirai, a frappé en octobre 2016 le service Dyn, qui sert à associer les noms de domaine aux adresses IP. De nombreux sites (Airbnb, Twitter, Reddit…) ont été rendus inaccessibles durant plusieurs heures. En cause, une armada de 100 000 appareils piratés (essentiellement des caméras) qui a noyé la plateforme sous les requêtes (ce que l'on appelle : attaque par déni de service ou DDoS). En septembre, Mirai s'était déjà attaqué à l'hébergeur français OVH, atteignant un trafic de 1,5 téra-octet (To) par seconde. De quoi faire tomber n'importe quel site en quelques minutes.

Cinq nouveaux objets recrutés par minute

Pour faire grossir ses rangs, le malware (un logiciel essayant d'infecter un ordinateur) scanne automatiquement des milliers d'adresses IP à la recherche d'objets connectés (caméras, imprimantes, routeurs…), puis teste une série d'identifiants par défaut pour infiltrer l'appareil. **« Il faut moins de trois minutes à un hacker pour prendre le contrôle d'un nouvel objet mis en réseau »**, indique ForeScout, une société spécialisée dans la sécurité de l'Internet des objets (IoT). Mirai infecterait cinq nouveaux objets par minute, avertit de son côté McAfee.
Ces botnets surpuissants auront bientôt la puissance nécessaire pour faire tomber l'intégralité d'Internet, s'inquiètent les experts. Avec un débit de 10 To par seconde, on peut paralyser un câble sous-marin. Le Liberia a ainsi vu tout son réseau bloqué par intermittence pendant plusieurs jours en novembre dernier. **« Le DDoS a tué notre activité économique »**, s'est lamenté un employé du principal opérateur mobile du pays…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation 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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

ou suivez nous sur

Réagissez à cet article

Source : *Les objets connectés vont faire sauter Internet – Edition du soir Ouest France – 06/06/2017*