**Media alert**

***Les principaux résultats du projet de recherche loT de Sophos***

**1500 tentatives d’accès à la ‘Maison Hantée’ par jour**

*Sophos a publié les résultats de son projet de recherche de cybersécurité ‘Maison Hantée’ IoT dans un whitepaper. La principale conclusion : aucun pirate n’a attaqué un équipement IoT implémenté, mais les tentatives d’accès se font de jour en jour plus fréquentes.*

Bruxelles, 27 novembre 2017 – **Les ‘Appareils du futur’ seront de plus en plus intelligents – en fait, ils les ont déjà. Ils communiquent sur la toile avec le monde entier et sont conçus pour nous divertir et nous faciliter la vie. Même si la plupart des utilisateurs savent qu’il faut sécuriser les ordinateurs, portables ou smartphones, ils ne sont pas suffisamment conscients des problèmes que peuvent poser les objets de leur Smart-Home.**

**La ‘Maison hantée’ : la simulation d’un Smart-Home**Jusqu’ici, il y a eu très peu d’informations au sujet de l’accès externe aux équipements loT. C’est pourquoi Sophos a créé, en collaboration avec Koramis, une infrastructure ​Smart-Home faisant office « d’appât » sur internet. La maison virtuelle est représentative d’un ménage normal, avec treize objets loT différents et des technologies provenant de différents fournisseurs qui sont tous connectés au même réseau.

**Les trois phases test**Les techniques et tentatives d’accès aux éléments d’objets implémentés ont été suivies lors de deux des trois phases test. La première phase de six semaines avait des mots de passe privés sécurisés. La deuxième phase de trois semaines visait un objectif identique, toutefois en utilisant les paramètres standard des équipements – tels que ceux que la plupart des ménages disposant d’équipements IoT utilisent. Pour examiner les résultats dans un contexte plus large, la troisième phase de recherche intégrait des scans actifs d’Internet pour les éléments d’objets IoT via des moteurs de recherche, tels SHODAN et Censys. Les résultats de ces scans sont visualisés dans ce que l’on nomme des *heat maps* ou cartographies d’activités.

**Les résultats alarmants, mais qui n’ont rien de surprenant**Les tentatives d’accès ont été plus nombreuses, voire nettement plus nombreuses, que prévu. Les tentatives provenaient de quasiment tous les pays du monde. Elles concernent au moins une tentative d’accès aux objets IoT de la Maison Hantée. On a enregistré au moins 1500 tentatives d’accès par jour aux équipements ayant un mot de passe sécurisé (et jusqu’à 3.800 avec les paramètres standard).

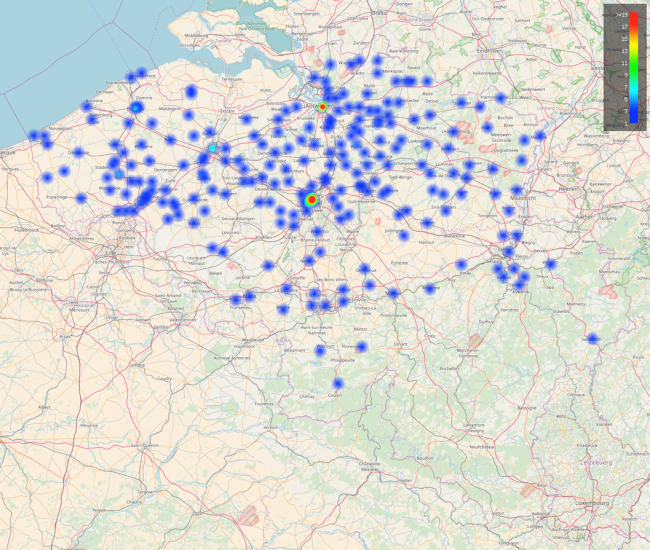
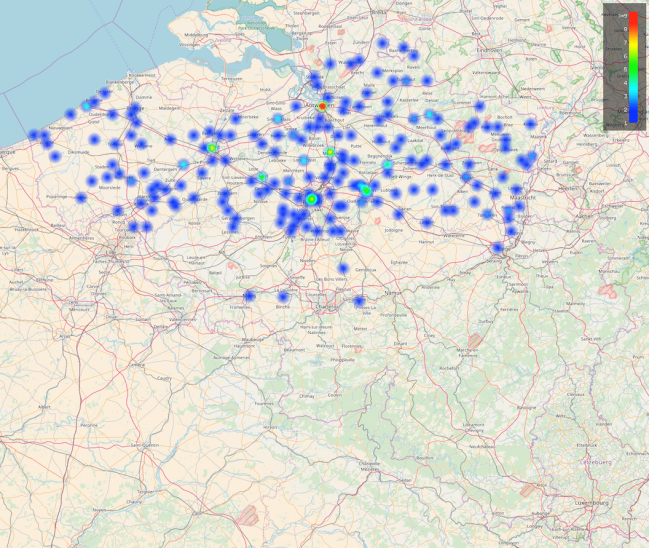
En examinant la cartographie, force est de constater que la Chine, les Etats-Unis et le Mexique figurent dans le top 3 des pays d’où proviennent des tentatives d’accès. Pour une description détaillée du projet de recherche Maison Hantée et les résultats, cliquez [**ici**](https://www.sophos-events.com/smarthome/en/index.cfm).

**La situation en Belgique**Des scans actifs d’internet ont été pris les 19 septembre 2017 et 14 novembre 2017. Ils ont révélé que, pour les systèmes examinés BacNet, Fox et KNX/IP, au total 507 (durant la première phase) et 534 (durant la deuxième phase) de ces systèmes sont accessibles depuis internet. Ces systèmes (réseaux) peuvent être détectés par Sophos et donc aussi par des personnes mal intentionnées. Pour la Belgique, il s’agit donc d’une croissance de plus de 5 % entre les deux dates des scans. Cette constatation s’aligne sur celle faite dans d’autres pays.

Les systèmes examinés ici (BacNet, Fox et KNX/IP) sont des systèmes d’automatisation de bâtiments et/ou de domotique, tel l’iPad contre le mur qui permet de régler la température ambiante, d’ouvrir et de fermer les rideaux, d’allumer la lumière, de régler les caméras de vidéosurveillance, etc.

Le 14 novembre, on a aussi examiné le nombre de pages web auxquels les appareils intelligents étaient connectés et qui peuvent également être détectés aisément, pas nécessairement des réseaux domestiques, mais aussi des pages Web d’un fabricant permettant de se connecter à un appareil intelligent. Citons, comme exemple, les pages Web auxquelles qui permet de se connecter aux caméras domestiques et qui permettent de voir de qui se passe chez eux ou dans leur jardin.

**Des cartes d’activités qui en disent long**  
Sur les cartes d’activités, on peut voir où se trouvent, en Belgique, ces réseaux dans les Smart-Homes et où l’on trouve, en Belgique, des systèmes d’interface web. Chaque point bleu représente au moins 1 appareil. Rouge est égal à plus de 9 appareils (interfaces) ou 19 réseaux (Smart-Home). Tous ces systèmes sont accessibles par internet.

Réseaux Smart-Homes Interfaces Web  
 

On trouve donc, au total, sur la première carte plus de 500 réseaux Smart-Home et sur la deuxième plus de 300 appareils qui sont tout simplement accessibles via internet par le biais d’un site web.

C’est dire combien les Belges sont négligents quand il s’agit d’appareils IoT et à quel point ce phénomène est généralisé. Autre constatation : les réseaux Smart-Home détectés se concentrent surtout en Flandre, avec des fortes concentrations à Bruxelles et Anvers, suivies de Gand, Bruges et Courtrai.  
**Pour tout complément d’information, contactez** Sandra Van Hauwaert, Square Egg, [sandra@square-egg.be](mailto:sandra@square-egg.be), GSM 0497 251816