**L’étude « Haunted House » de Sophos dévoile les risques encourus avec les objets connectés (IoT) domestiques**

* *L’étude révèle l’existence de plus de 70 000 tentatives d'accès à des Smart-Homes.*
* *La recherche d’équipements Smart-Home a répertorié plus de 68 000 interfaces accessibles depuis internet.*
* *869 interfaces accessibles depuis internet pour la Belgique, classe au 15ème rang.*

Bruxelles, 26 octobre 2017 - **Pour célébrer Halloween cette année, Sophos a lancé le projet « Haunted House », en collaboration avec le spécialiste de l'automatisation industrielle Koramis. Les résultats définitifs du projet de recherche seront publiés en novembre 2017. Cependant, les premiers chiffres provisoires ont dévoilé l’existence de plus de 70 000 tentatives d'accès, en provenance de 24 089 IPS (Intrusion Prevention System) individuelles, à notre maison virtuelle. Ainsi, une tendance claire est déjà évidente : le concept de « Haunted House » n'est pas lié uniquement à Halloween, mais devient un réel danger pour les Smart-Homes privées, si ces dernières ne sont pas sécurisées correctement.**

Pour appuyer ces chiffres et permettre une classification au niveau d’un périmètre plus large, le projet intègre également des scans actifs d’internet pour les objets connectés domestiques intelligents via des moteurs de recherche tels que Shodan ou Censys. Un scan, qui a débuté en octobre, a abouti à plus de 68 000 interfaces accessibles depuis internet, concernant des éléments d’objets connectés bien définis, et principalement utilisés dans des espaces privés, tels que des contacteurs de fenêtre sans fil, des détecteurs de fumée, des systèmes d'ouverture/fermeture automatique de porte, et enfin des caméras de vidéosurveillance. Tous ces équipements étaient facilement accessibles via internet. La visualisation, par le biais des cartographies d’activités, montre que la technologie IoT est concentrée dans les villes et les centres urbains, et a tendance à disparaître dans les zones rurales.

«Les chiffres soulignent l'importance d'être très prudent lors de la construction de votre Smart-Home», déclare Tim Stamer, Marketing Manager Benelux. "Sinon, il y a de grandes chances que ce ne soit pas juste des enfants qui frappent à votre porte pour Halloween, mais de vrais cybercriminels, intéressés sans aucun doute par votre argent et vos données".

**8 conseils pour éviter de finir dans une «Haunted-House», en gardant plutôt votre Smart-Home sécurisée :**

1. **Gardez vos réseaux domestiques privés**. Ne les partagez pas avec des tiers.
2. **Ne connectez pas vos objets connectés à votre réseau domestique si cela n'est pas nécessaire**. Par exemple, votre téléviseur ne doit pas être connecté au WLAN (réseau local sans fil), si vous regardez principalement la télévision via le câble ou une antenne.
3. **Créez un réseau séparé pour vos objets connectés**. Si votre routeur WiFi est capable de créer différents réseaux (segmentation), vous devriez créer un réseau spécial pour les objets connectés et interdire ainsi l'accès à votre réseau principal.
4. **Créez différents réseaux isolés au niveau de différents WLANs (réseaux locaux sans fil).** Il est même préférable de créer différentes zones réseau isolées pour le Home Office, les activités de divertissement, les divers aspects techniques ou liés à la sécurité ou encore le réseau invité, afin que toutes ces activités soient sur des WLANs différents. Cette mise en œuvre peut être facilitée et activée par un pare-feu qui permet seulement la communication nécessaire pour l’utilisation des composants, mais pas la propagation d'une infection d'un objet connecté à un autre. Vous pouvez installer Sophos XG Firewall Home Edition gratuitement sur votre PC.
5. **Utilisez la technologie VPN sécurisée**. Vous ne devriez pas utiliser les transferts via des ports non sécurisés, au niveau de votre routeur, pour accéder à distance à vos objets connectés, et ce depuis internet. Utilisez plutôt une technologie VPN sécurisée sur votre smartphone ou votre Mac/PC.
6. **Gardez votre logiciel à jour**. Installez un logiciel AV à jour sur tous vos PC, Mac et Smartphones Android. Des outils gratuits, tels que Sophos Home ou Sophos Mobile Security, sont disponibles sur le site internet de Sophos.
7. **Sécurisez tous vos équipements avec les dernières versions de firmwares**. Pas seulement votre PC, ordinateur portable ou vos smartphones. En effet, chaque objet connecté doit fonctionner avec le firmware le plus à jour, pour être le plus sécurisé possible. Ces précautions peuvent prendre du temps à mettre en place, mais le jeu en vaut la chandelle, surtout en matière de sécurité et de confidentialité.
8. **Et n’oubliez pas que Google est votre ami**. Vous pouvez faire une recherche sur Google concernant les failles de sécurité potentielles concernant l’objet connecté qui vous intéresse. Cette dernière peut ainsi vous donner un aperçu rapide, mais pertinent, sur l’intéret que les cybercriminels ont pour votre produit.

**A propose de Sophos**Sophos est un leader dans la sécurité des réseaux et des systèmes endpoint next-generation et, en tant que pionnier en matière de sécurité synchronisée, développe son offre innovante qui comprend des solutions pour le chiffrement, les systèmes endpoint, le web, les emails, les mobiles et les réseaux, afin de mieux travailler ensemble. Plus de 100 millions d’utilisateurs dans 150 pays font confiance à Sophos, et considèrent sa gamme complète de produits de sécurité informatique comme la meilleure solution pour se protéger contre les menaces complexes et la perte de données. Les produits Sophos sont disponibles exclusivement via un réseau mondial de plus de 26 000 partenaires enregistrés. Le siège social de Sophos se situe à Oxford (Royaume-Uni) et Sophos a été introduit à la bourse de Londres sous le nom SOPH. Plus d’informations sont disponibles sur [www.sophos.com](http://www.sophos.com).

**Contacts presse**Sandra Van Hauwaert, Square Egg, sandra@square-egg.be, GSM 0497251816