**Media alert**

***De belangrijkste resultaten van het Sophos IoT-onderzoek***

**1.500 toegangspogingen per dag in het ‘Haunted House’***Sophos heeft de resultaten van het IoT-beveiligingsonderzoek ‘Haunted House’ in een whitepaper verwoord. De belangrijkste conclusie: geen enkele hacker heeft een geïmplementeerd IoT-apparaat overvallen maar het aantal aanvallen nam elke dag toe.*

Brussel, 27 november 2017 – **‘Devices of the future’ zullen slim zijn of slimmer worden – en eigenlijk zijn ze dat nu al. Ze communiceren via internet met de hele wereld en ze zijn ontworpen om ons te amuseren en ons dagelijks leven te vergemakkelijken. Hoewel de meeste gebruikers al bekend zijn met IT-beveiliging voor computer, laptop en smartphone is het bewustzijn voor smart home-componenten onderbelicht.**

**Het ‘Haunted House’: smart home simulatie**Tot nu toe zijn gegevens over externe toegang tot IoT-apparatuur zeldzaam. Daarom heeft Sophos samen met Koramis een ​​smart home-infrastructuur opgezet die als ‘honey pot’ op het internet werd geplaatst. Het huis vertegenwoordigt een doorsnee privéhuishouden met dertien verschillende IoT-apparaten en technologieën van verschillende leveranciers, die zich in een netwerk bevinden en met internet zijn verbonden.

**Drie testfasen**Binnen twee van de drie testfasen werden de technieken en het aantal toegangspogingen tot de geïmplementeerde componenten gevolgd. De eerste fase duurde zes weken met persoonlijke en veilige wachtwoorden. De tweede fase met eenzelfde opzet duurde drie weken. Het verschil: er werden standaardinstellingen voor apparaten gebruikt – net zoals het zeer waarschijnlijk is bij huishoudens die IoT-apparaten gebruiken. Om deze resultaten in een grotere context te krijgen, paste een derde onderzoeksfase actieve internetscans toe voor open IoT-componenten. Hierbij werden zoekmachines als SHODAN en Censys ingezet. De resultaten van deze scans worden in zogenaamde *heat maps* gevisualiseerd.

**De resultaten: niet verrassend maar alarmerend**De toegangspogingen waren hoger dan verwacht en vielen erg hoog uit. Uit bijna elk land wereldwijd werd er op zijn minst één keer geprobeerd om verbinding te leggen met een van de IoT-apparaten in het Haunted House. Terwijl er met veilige wachtwoorden werd gewerkt, werden dagelijks 1.500 toegangspogingen vastgelegd (en zelfs 3.800 met de standaardinstellingen).

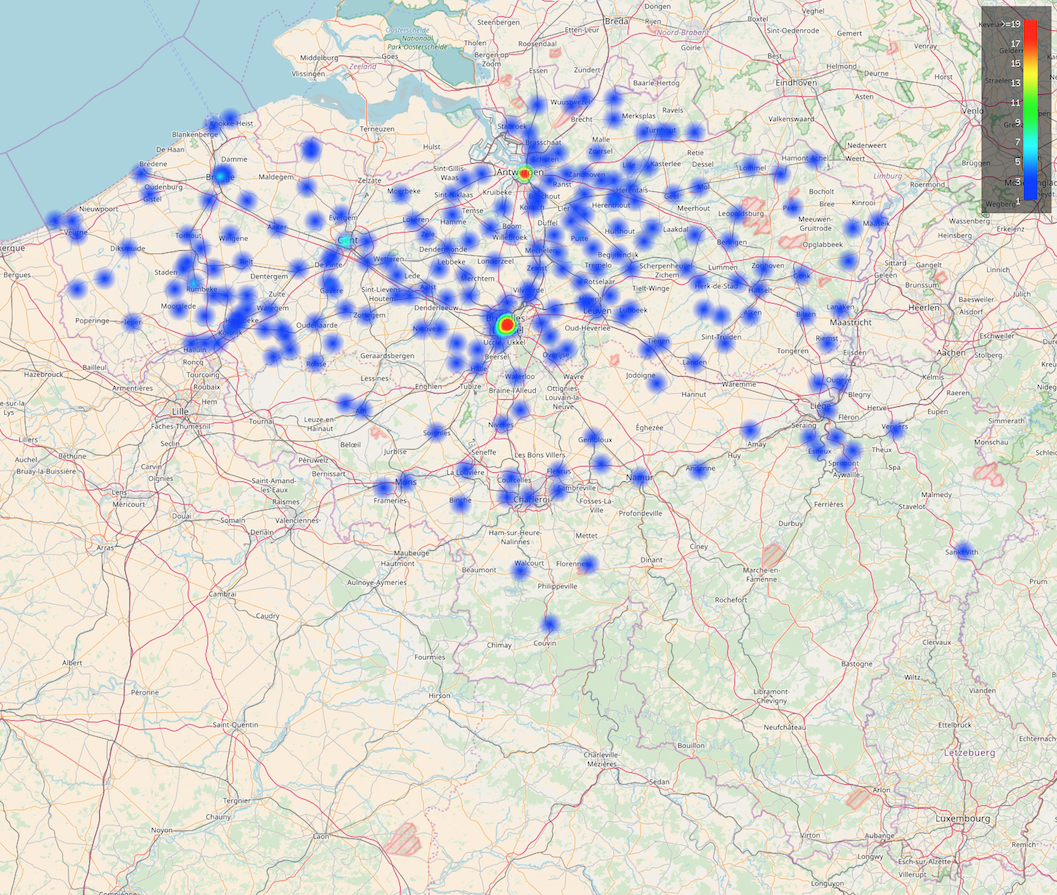
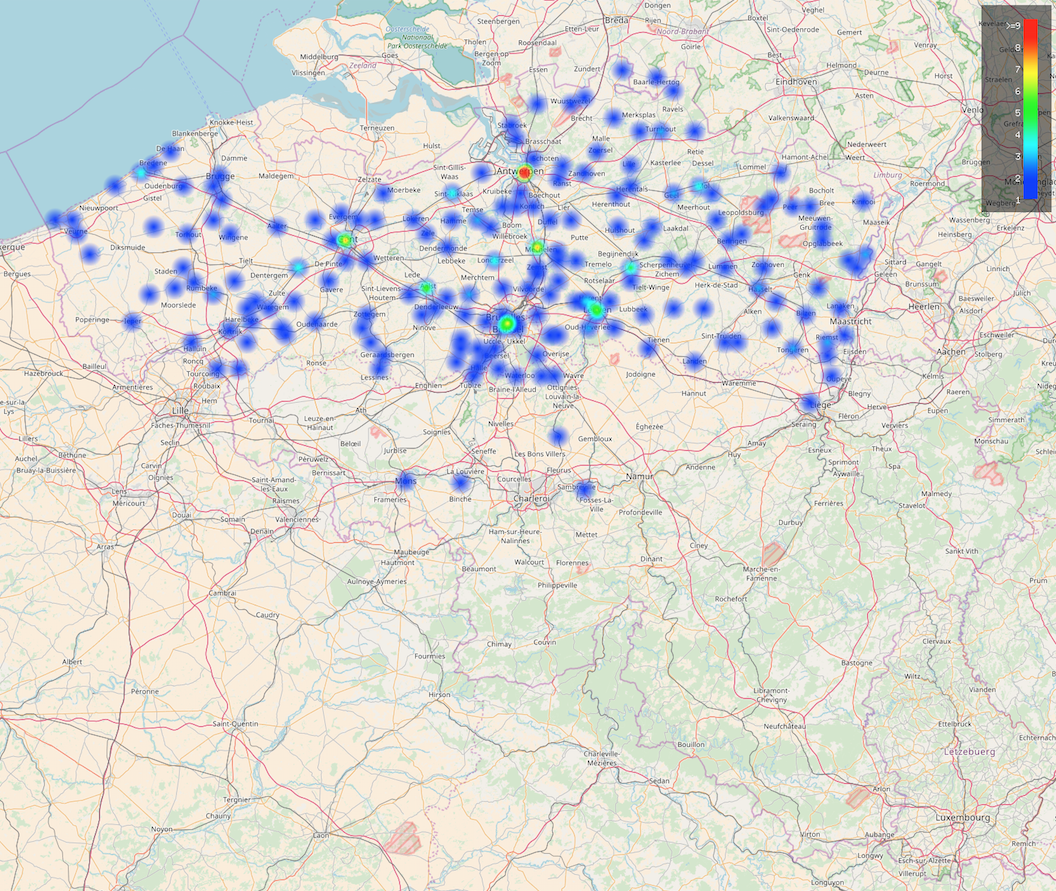
Wordt er gekeken naar de verschillende landen, staan ​​China, de VS en Mexico in de top drie van de landen waar de toegangspogingen vandaan kwamen. Een gedetailleerde beschrijving van de Haunted House-studie inclusief resultaten is [**hier**](https://www.sophos-events.com/smarthome/en/index.cfm) te vinden.

**Specifiek voor België**De actieve internetscans in België vonden plaats op 19 september 2017 en op 14 november 2017. Daaruit is gebleken dat voor de onderzochte systemen BacNet, Fox en KNX/IP, in totaal 507 (in een eerste fase) en 534 (in een tweede fase) systemen open aan het internet zijn verbonden. Deze systemen (netwerken) zijn vindbaar voor Sophos en dus ook voor criminelen. In België betekent dit een groei van meer dan 5% tussen de twee meetmomenten. Dit is in lijn met de bevindingen in andere landen.

De systemen die hier zijn bekeken (BacNet, Fox en KNX/IP), zijn bedoeld voor gebouw-automatisering en/of domotica. Denk bv. aan een iPad aan de muur waarmee je de temperatuur van de chauffage kunt regelen, gordijnen kunt sluiten, licht kunt aansteken, camera’s kunt bedienen, etc.

Op 14 november is ook gekeken naar het aantal webpagina’s waaraan smart devices gekoppeld zijn en die ook gemakkelijk vindbaar zijn. Dat zijn niet persé thuisnetwerken maar kunnen evengoed webpagina’s zijn van een fabrikant waarbij je kunt inloggen op een smart home device. Voorbeelden hiervan zijn webpagina’s waar je kunt inloggen op camera’s bij mensen thuis om mee te kijken in de huiskamer of tuin.

**Extra duiding bij de kaarten**  
Op de kaarten is te zien waar in België die netwerken in smart homes te vinden zijn en waar in België systemen met web gui’s te vinden zijn. Ieder blauw stipje is minimum 1 apparaat. Rood betekent respectievelijk meer dan 9 (web gui) apparaten of 19 (smart home) netwerken. Al deze systemen zijn open aan het internet verbonden.

Smart homes netwerken Web gui’s  
 

In totaal staan dus op de ene kaart meer dan 500 smart home netwerken en op de andere kaart meer dan 300 apparaten die door middel van een website zomaar vrij toegankelijk bereikbaar zijn vanaf het internet.

Het geeft een duidelijk beeld van hoeveel mensen er nonchalant met IoT-apparaten omgaan in België, en hoe wijd dit in ons land verspreid is. Bovendien is duidelijk te zien dat de gevonden smart home netwerken zich vooral concentreren in Vlaanderen, met uitschieters in Brussel en Antwerpen, daarna komen Gent, Brugge en Kortrijk.  
**Voor meer informatie:**Sandra Van Hauwaert, Square Egg, [sandra@square-egg.be](mailto:sandra@square-egg.be), GSM 0497 251816