IoT, uma oportunidade ou uma ameaça para as Casas Inteligentes?

Sophos revela os principais resultados do seu estudo sobre segurança em dispositivos IoT, o "Haunted House"

Lisboa, 6 de dezembro de 2017 - Os dispositivos do futuro serão inteligentes: vão comunicar com o mundo exterior através da Internet, oferecendo-nos entretenimento e facilitando as tarefas maçadoras do dia-a-dia. Mas ainda que os utilizadores já estejam conscientes da importância de proteger os seus computadores ou dispositivos móveis, esta sensibilização ainda está muito aquém quando falamos de dispositivos para casas inteligentes – ainda que estes dispositivos IoT compatíveis com Web, sejam nada mais nada menos que pequenos computadores dentro da própria rede do utilizador.

A "*Haunted House*" – a simulação de uma casa inteligente

A Sophos, em parceria com a Koramis, criou a infraestrutura de uma casa inteligente como um sistema deteção de intrusos (*honeypot*): a "**Haunted House**". Numa superfície de 4 x 2,5 metros, desenhada para parecer um apartamento, foram instalados 13 dispositivos IoT e sistemas de controlo de diferentes fabricantes, ligados e conectados à Internet – à semelhança do que se faz atualmente nas residências mais modernas.

Três fases de teste

Em duas das três fases de teste, foi registado a natureza e a frequência das tentativas para aceder aos dispositivos da Haunted House. A primeira fase foi realizada com passwords seguras criadas especificamente para o teste, durante seis semanas. A segunda fase com a mesma metodologia durou três semanas, mas com as configurações predefinidas dos fabricantes – tal como costumamos ver nos dispositivos instalados em residências privadas.

Para permitir a classificação destes resultados num contexto mais amplo, uma terceira fase foi levada a cabo com objetivo de realizar verificações de Internet ativas para dispositivos IoT típicos e abertos através de motores de busca de IoT, SHODAN e Censys. Os resultados foram representados num "mapa de calor" para a região de Portugal e Espanha, e o resto do mundo (am anexo).

Os resultados: pouco surpreendentes, mas alarmantes

O número de tentativas para aceder à Haunted House foi elevado, excedendo às nossas expectativas. Desde quase todos os países do mundo surgiu pelo menos uma tentativa de contacto com um dispositivo IoT presente na casa, durante o período de teste:

- Na primeira fase, que decorreu na primavera de 2017, registou-se aproximadamente **1.500 tentativas diárias de acesso**;
- Na segunda fase, no outono de 2017, foram registadas **3.800 tentativas**.

A distribuição das tentativas de acesso desde países individuais difere nas duas fases de teste. Enquanto que a China e os EUA ocupam os primeiros lugares do pódio, o país em terceiro lugar muda drasticamente: apesar de surgir em 3º lugar na primeira fase, o México não aparece nem no Top 10 na segunda fase. O Brasil, que se situa em 5º lugar na primeira fase, ocupa o lugar deixado pelo México na segunda fase.

O mais surpreendente é que no segundo período de apenas três semanas, foi possível identificar 27 tentativas diretas de acesso. É possível deste modo concluir que na fase em que as configurações standard prevaleciam, em média mais convidados indesejados visitaram a Haunted House por dia. Não foram feitas alterações nos sistemas – embora tivesse sido possível.

As verificações de Internet ativas revelaram várias portas de acesso de Internet para os dispositivos de IoT, com uma tendência crescente. Na região da Península Ibérica, verificou-se **um aumento dos pontos de acessos de 3,3%** até os 1.549 em apenas dois meses – de meados de setembro a meados de novembro. Esta taxa é ligeiramente mais alta que a média anual de crescimento - 3,1%.

A descrição detalhada do estudo "Haunted House" e dos resultados foram publicados num white paper que pode ser descarregado em www.sophos-events.com/smarthome/.

Como nos podemos proteger?

"Em primeiro lugar, o utilizador deve ter em mente que muitos dispositivos IoT são computadores de pequenas dimensões e compatíveis com Web, que podem ser controlados desde o exterior", diz Michael Veit, IT Security Expert na Sophos. Por isso, se pretende evitar que hackers acedam aos seus ficheiros ou utilizem o poder de processamento dos seus dispositivos para realizar ciberataques de grande escala, deve tem em conta algumas dicas:

- A minha casa é o meu castelo: nunca partilhar a sua rede doméstica com ninguém
- Faça uma simples pesquisa na Internet para descobrir como aceder ao nível de segurança do dispositivo IoT / para casa inteligente em questão
- Altere as passwords que vêm por defeito com passwords seguras logo que o dispositivo é instalado

- Se existem atualizações disponíveis (este é um pré-requisito de segurança), faça sempre as atualizações de firmware
- Sempre que possível retire os dispositivos IoT da sua rede doméstica. Um exemplo: se o seu sinal de televisão é recebido principalmente por cabo ou antena, a sua televisão pode funcionar sem acesso à internet sem fios.
- Na sua rede doméstica, faça uma distinção entre dispositivos importantes e não importantes. Estes devem ser configurados em redes diferentes para assegurar que dispositivos não seguros não têm acesso à informação confidencial.
- Áreas de rede "seladas": o mais seguro é criar áreas de rede "seladas" para o escritório em casa, para eletrodomésticos de consumo, para sistemas de construção e segurança e para a rede dos convidados com diferentes redes sem fios. Isto é possível através de uma firewall que apenas permite a comunicação necessária para utilizar os dispositivos, evitando uma infeção de se espalhar de um dispositivo IoT para outro. A firewall Sophos XG Firewall Home Edition pode ser descarregada gratuitamente.
- Utilize tecnologia VPN segura: em vez de permitir acesso remoto da Internet ao dispositivo IoT configurando o reencaminhamento de porta não seguro no router, é mais prudente utilizar a tecnologia VPN no seu smartphone ou Mac/PC.
- Evidentemente, os dispositivos "tradicionais" como PCs, smartphones e portáteis devem estar protegidos com softwares antivírus. Existem versões gratuitas disponíveis, por exemplo, em www.sophos.com/freetools.

###

Sobre a Sophos

A Sophos é uma empresa líder em soluções de segurança de *'next generation'* na rede e para *endpoint*. Enquanto pioneira na área da segurança sincronizada, a Sophos desenvolve um portfólio de soluções de segurança inovadoras para *endpoint*, rede, encriptação, web, email e mobile que trabalham perfeitamente em conjunto. Mais de 100 milhões de utilizadores em 150 países confiam nas soluções Sophos como a melhor proteção contra ameaças sofisticadas e perda de informação. Os produtos Sophos estão exclusivamente disponíveis através de um canal global com mais de 26.000 parceiros registados. A Sophos está sediada em Oxford, no Reino Unido e está cotada em bolsa na Stock Exchange de Londres, sob o símbolo "SOPH." Mais informação disponível em http://www.sophos.com/.

Siga a Sophos nas redes sociais: Twitter, LinkedIn, Facebook, Spiceworks, YouTube, Google+

Para mais informação, por favor contacte:

LEWIS

Nanci Martinez
910 939 847
nanci.martinez@teamlewis.com

Ana Luzia
914 377 330
ana.luzia@teamlewis.com