A CIA pode ouvir o que se fala pelas smart TVs? Entenda e previna-se

Tecnologia

Enviado por: folhagospel

Enviado em: 10-03-2017

300) this.width=300" />

Antes consideradas uma ótima maneira de relaxar em casa, as TVs inteligentes conectadas à internet, ou smart TVs, agora viraram motivo de preocupação.

O vazamento mais relevante sobre espionagem digital dos últimos tempos revelou que a agência de inteligência americana, a CIA, conta com um arsenal de ferramentas hackers e explora falhas de segurança do tipo "dia zero" (jargão para falhas desconhecidas pelos fabricantes). Com softwares e vírus, consegue interceptar mensagens de aplicativos como WhatsApp e Telegram, grampear conversas, vasculhar computadores... e invadir os microfones das smart TVs da Samsung.

O documento do WikiLeaks cita um mecanismo para comprometer os televisores modelo F8000 chamado "Weeping Angel" ("Anjo chorão", em português).

Com data de junho de 2014, o conteúdo descreve a criação de um modo de "falso desligado" nos aparelhos, criado para enganar os usuários e fazê-los acreditarem que as telas não estão em funcionamento, enquanto acontece a gravação secreta do áudio captado pelas TVs.

As conversas seriam transmitidas pela internet para servidores da CIA assim que as televisões voltassem a ser ligadas.

Após um primeiro comunicado curto sobre o assunto, em que reforçou a privacidade dos consumidores e a segurança dos seus produtos como prioridade, a Samsung emitiu uma versão

mais completa.

"O relatório descreve um software malicioso, instalado por meio de uma unidade USB e que se aplica a firmwares em TVs vendidas em 2012 e 2013, a maioria das quais já foram corrigidas por meio de uma atualização de firmware. (...) Monitoramos continuamente os riscos de segurança em todas as nossas plataformas de Smart TV e, se encontrarmos um risco, cuidamos imediatamente. A melhor ação que os consumidores podem tomar para garantir a segurança de qualquer dispositivo é manter sempre seu software e aplicativos atualizados", disse a empresa.

Toda smart TV conta com suas próprias configurações e regras para coletar áudios e outras informações pessoais --como localização e quantas vezes a TV é ligada, por exemplo. As informações são usadas pelas fabricantes para "saber mais" sobre seus consumidores e, em tese, melhorar os serviços e produtos.

Você pode desligar esses recursos se quiser, mas para isso precisará fuçar nas configurações de cada aparelho.

Há algum tempo, ficamos sabendo que o dono do Facebook, Mark Zuckerberg, cobre a câmera e o microfone do seu computador com uma fita adesiva por precaução. Você pode tentar fazer isso na smart TV se souber onde fica o microfone, mas a localização varia conforme o modelo e nem sempre é fácil de achar; o manual de instruções pode te ajudar nesta tarefa. É algo que não deve interferir nas funções básicas da TV.

História repetida

A própria Samsung esteve na berlinda por causa disso há dois anos, quando afirmou não "espionar" os usuários, em um comunicado similar ao desta semana. Na época, a política de privacidade das suas TVs gerou polêmica.

"Por favor, leve em conta que se suas palavras faladas incluem informação pessoal ou confidencial, esta fará parte dos dados capturados e transmitidos a um terceiro através do uso da função de reconhecimento de voz", dizia o documento.

Em fevereiro deste ano, a empresa norte-americana Vizio teve que pagar uma multa de US$ 2,2 milhões em um acordo com o órgão regulatório do comércio dos EUA depois de coletar dados dos usuários de 11 milhões de suas smart TVs sem eles saberem o que estava acontecendo.

Quer dizer, se a CIA vai ouvir o que estamos falando não dá para saber, mas o fato é que estamos vulneráveis.

Para Camillo di Jorge, presidente da empresa de segurança digital ESET no Brasil, o problema com as TVs inteligentes é algo que deve crescer com a penetração cada vez maior da chamada Internet das Coisas, com objetos conectados e cada vez mais inteligentes.

"Se vai conectar uma TV à internet ou o celular a uma rede desconhecida, vai correr riscos", diz, reforçando que não existe um sistema 100% seguro.

Segundo ele, além de desligar a captura de voz da TV, você deve tomar cuidado com as informações que você expõe, via voz, aos dispositivos.

Além disso, é recomendável manter atualizados os sistemas operacionais das TVs, que corrigem eventuais falhas de segurança à medida que forem surgindo, e evitar comprar aparelhos de marcas pouco confiáveis.

Em último caso, se quiser ter certeza de que não será vigiado, a opção é desconectar a rede Wi-Fi de sua smart TV, embora com isso sua TV vai deixar de ser "smart" e perderá o acesso a conteúdos da internet.

Fonte: UOL Tecnologia