Quinta-Feira, 04 de Junho de 2026

Robôs aspiradores são hackeados nos EUA e insultam proprietários; entenda o caso

Robôs aspiradores da marca Ecovacs, modelo Deebot X2, foram hackeados em diversas cidades dos Estados Unidos, permitindo que invasores controlassem os dispositivos remotamente e proferissem insultos raciais e obscenidades por meio de seus alto-falantes. Os incidentes ocorreram em um intervalo de poucos dias e expuseram falhas de segurança no modelo, que já haviam sido alertadas por pesquisadores de segurança cibernética meses antes.

Daniel Swenson, um advogado de Minnesota, relatou ao site australiano ABC News que seu robô aspirador começou a funcionar de forma errática enquanto ele assistia televisão. Ao verificar o aplicativo Ecovacs em seu celular, Swenson percebeu que um estranho estava acessando a câmera do dispositivo e o controlando remotamente.

Após redefinir a senha e reiniciar o robô, o dispositivo foi novamente controlado pelo invasor, que passou a proferir insultos raciais através dos alto-falantes, na frente do filho de 13 anos de Swenson.

Outros casos semelhantes foram relatados em diferentes cidades dos EUA. Em Los Angeles, no mesmo dia do incidente em Minnesota, um robô aspirador Deebot X2 perseguiu o cachorro de seu dono enquanto emitia comentários abusivos. Cinco dias depois, em El Paso, outro dispositivo começou a proferir insultos raciais durante a noite, até ser des

Falhas de segurança conhecidas

As falhas de segurança que permitiram os ataques já haviam sido identificadas por pesquisadores de segurança cibernética em dezembro de 2023. Dennis Giese e Braelynn Luedtke, demonstraram durante uma conferência como o sistema de código PIN que protegia o acesso remoto ao dispositivo e à câmera podia ser facilmente contornado.

Os pesquisadores descobriram que o código PIN de segurança era verificado apenas pelo aplicativo, e não pelo servidor ou pelo robô. Isso significa que qualquer pessoa com conhecimento técnico poderia contornar a verificação e acessar o dispositivo e sua câmera remotamente. Eles alertaram a Ecovacs sobre o problema antes de divulgar a falha publicamente, mas a empresa não corrigiu a vulnerabilidade de forma satisfatória.

A Ecovacs, fabricante dos robôs aspiradores, confirmou os ataques e informou que uma atualização de segurança seria lançada em novembro. A empresa, no entanto, negou que seus sistemas tenham sido comprometidos diretamente e atribuiu os incidentes ao “credential stuffing”, uma técnica em que hackers utilizam credenciais de login vazadas de outros sites e serviços para tentar acessar contas em diferentes plataformas.

Os incidentes geraram preocupações sobre a privacidade dos usuários, já que os robôs aspiradores possuem câmeras e microfones que podem ser acessados remotamente. Especialistas em segurança alertam para a importância de utilizar senhas fortes e únicas para cada serviço online, além de proteger as redes Wi-Fi com senhas mais robustas além da criptografia.

fonte leiaja