Hackers violan cámaras de seguridad en cárceles, bancos y hospitales de EEUU

Un grupo de piratas informáticos, liderados por Tillie Kotman, afirmaron haber violado un tesoro de datos de cámaras de seguridad recopilados por la startup de Silicon Valley Verkada.

Los delincuentes obtuvieron acceso directo a transmisiones en vivo de más de 100.000 cámaras de vigilancia dentro de hospitales, empresas, prisiones, escuelas y departamentos de policía en Estados Unidos.

Otras empresas expuestas fueron la fabricante de automóviles Tesla y el proveedor de software Cloudflare. Asimismo, los hackers accedieron a vídeos desde el interior de las clínicas de salud para mujeres, hospitales psiquiátricos y oficinas de empresas que desarrollan equipos de seguridad.

En los últimos años, la ola de ataques cibernéticos ha hecho saltar las alarmas en el continente europeo. Tan solo en el último año, se han realizado más de 40.000 ciberataques al día en España.

Sin embargo, las bandas organizadas ya no solo enfocan sus técnicas en el sector empresarial, sino también dentro de los hogares inteligentes. “Actualmente, el hackeo de dispositivos móviles y otros elementos conectados en el hogar ya es una realidad.

Frente a este escenario, el 70% de los usuarios en España consideran indispensable contar con un sistema de ciberseguridad en el hogar, con el objetivo de proteger sus dispositivos durante el teletrabajo.

Por otro lado, diversos estudios han demostrado que las cámaras webs y termostatos inteligentes pueden convertirse en un objeto atractivo para los ciberdelincuentes”, apunta el especialista en domótica de ElDulceHogar, Mauricio Orbegoso.

En un vídeo visto por Bloomberg, una cámara de de Verkada dentro del hospital de Florida Halifax Health mostró lo que parecían ser ocho empleados dentro del hospital abordando a un hombre e inmovilizando contra una cama.

El hospital apareció en el sitio web público de Verkada en un

estudio de caso titulado: “Cómo un proveedor de atención médica de Florida actualizó e implementó fácilmente un sistema de seguridad escalable compatible con HIPAA”.

En el caso de Tesla, otro vídeo muestra a un grupo de trabajadores en una línea de ensamblaje dentro de un almacén de la empresa en Shanghái, China. Según indicaron los piratas informáticos, la información se obtuvo con el acceso a 222 cámaras en las fábricas y almacenes de la compañía de Elon Musk.

Finalidad del ciberataque

La violación de datos la realizó un colectivo de piratas informáticos internacional. El grupo, liderado por Tillie Kottmann, tuvo como objetivo mostrar la omnipresencia de la videovigilancia y la facilidad con la que pueden ingresar a los sistemas de diversas instituciones.

Kottmann, que utiliza pronombres de ellos/elles, se atribuyó el crédito por piratear al fabricante de chips Intel y a Nissan Motor. A su vez, dijo que las razones para piratear son “mucha curiosidad, luchar por la libertad de información y contra la propiedad intelectual, una gran dosis de anticapitalismo, una pizca de anarquismo”.

Con Información de La Verdad