Desde hace unas semanas el software de videoconferencias Zoom ha aumentado su popularidad considerablemente, debido al brote del coronavirus, pues ha servido de mucho para quienes hacen videoconferencias de trabajo o imparten clases en línea, lo que ha ayudado a la compañía a contar con 200 millones de usuarios al día, de un promedio de tan solo 10 millones en diciembre pasado.

Sin embargo, este aumento exponencial de usuarios ha causado problemas derivadas de fallas de seguridad en el software de Zoom. La compañía no había planeado llegar a más allá de usuarios empresariales, pero debido a la pandemia del COVID-19, ahora se utiliza de muchísimas maneras diferentes, lo que ha llamado la atención de hackers.

De acuerdo con publicaciones de The Guardian, algunos expertos aseguran que Zoom es una pieza legítima de software, pero desafortunadamente, tiene muchas vulnerabilidades de seguridad y ahora se están conociendo.

La política de privacidad de Zoom fue criticada por hacer posible la recopilación de datos extensos acerca de los usuarios, como videos, transcripciones y notas compartidas, y luego compartirlos con terceros para beneficio personal. El 29 de marzo, Zoom endureció su política de privacidad para asegurar que no utiliza datos de reuniones para ninguna publicidad. Pero sí utiliza los datos cuando las personas visitan sus sitios web de marketing, incluidas sus páginas de inicio Zoom.us y Zoom.com.

La aplicación de Zoom, como muchas otras, utiliza el SDK de Facebook, y se encontró enviando datos analíticos a la red social, aún cuando el usuario no tiene una cuenta de Facebook vinculada. Después, Zoom eliminó la función.

Zoom pasó por debajo de la lente por su función de *«seguimiento de asistentes»*, que al estar habilitada, permite al anfitrión verificar si los participantes hacen clic fuera de la ventada principal de Zoom durante una llamada. El 2 de abril, la compañía eliminó permanentemente la función de seguimiento de atención de los asistentes. Un anfitrión de una reunión de Zoom también puede leer mensajes de texto privados enviados durante una llamada si se graba localmente.

Hace poco, investigadores de seguridad cibernética descubrieron una falla en la aplicación de Windows de Zoom, que la hizo vulnerable a inyección de ruta UNC que podría permitir que los hackers remotos roben credenciales de inicio de sesión de Windows de las víctimas e incluso ejecutar comandos arbitrarios en sus sistemas.

El 2 de abril, se emitió un parche para abordar dicha falla y otros dos errores reportados por Patrick Wardle, que permiten a los atacantes obtener privilegios de root y acceder al micrófono y la cámara en macOS, permitiendo así grabar las reuniones de Zoom.

Además, se encontró que Zoom estaba utilizando una función de minería de datos no revelada, que combinaba de forma automática los nombres de usuarios y direcciones de correo electrónico con sus perfiles de LinkedIn cuando iniciaban sesión, aún cuando eran anónimos o utilizaban un seudónimo en su llamada. Si otro usuario en su reunión se suscribió a un servicio llamado LinkedIn Sales Navigator, es posible que los atacantes pudieran acceder a los perfiles de LinkedIn de otros participantes en sus reuniones de Zoom sin el conocimiento o consentimiento de los usuarios. Como respuesta, Zoom también deshabilitó esta función.

El medio Vice reveló que Zoom está filtrando las direcciones de correo electrónico y fotos de miles de usuarios, además de permitir que extraños intenten iniciar llamadas entre ellos. Esto se debe a que los usuarios con el mismo nombre de dominio en su dirección de correo electrónico (proveedores de correo electrónico no estándar que no son Gmail, Outlook, Hotmail o Yahoo!), se agrupan como si trabajaran para la misma empresa. Debido a esto, Zoom incluyó en lista negra estos dominios.

Por otro lado, el 3 de abril de 2020, el Washington Post informó que era trivial encontrar grabaciones de video realizadas en Zoom al buscar el patrón común de nombres de archivos que Zoom aplica de forma automática. Estos videos se encontraron en cubos de almacenamiento de Amazon de acceso público.

En otro suceso, los investigadores creaeron una nueva herramienta llamada *«zWarDial»*, que busca ID de reunión Zoom abierta, y encontraron alrededor de 100 reuniones por hora que

no están protegidas por ninguna contraseña.

Las afirmaciones de Zoom sobre su uso del cifrado de extremo a extremo para asegurar las comunicaciones demostraron ser engañosas. La compañía declaró que en una reunión en la que cada participante utiliza un cliente Zoom y que no está grabando, todo tipo de contenido (video, audio, pantalla compartida y chat), se cifra en el lado del cliente y nunca se descifra hasta que llega a los otros receptores. Pero si uno de los servicios de valor agregado, como la grabación en la nube o la telefonía de marcado, está habilitado, Zoom tiene acceso a las claves de descifrado, que actualmente mantiene en la nube. Esto también facilita que los *«piratas informáticos o una agencia de inteligencia del gobierno obtengan acceso a esas claves»*, dijo el experto en seguridad cibernética Matthew Green.

Una investigación posterior, realizada por Citizen Lab, descubrió que también la compañía utilizaba un tipo de cifrado muy vago, con las claves generadas por las operaciones criptográficas *«entregadas a los participantes en una reunión de Zoom por medio de servidores en China, incluso cuando los participantes de la reunión, y la compañía del suscriptor de Zoom, están fuera de China».* El audio y el video en cada reunión de Zoom se cifran y descifran con un solo AES-128 utilizado en modo ECB que se comparte entre todos los participantes. No se recomienda el uso del modo ECB porque los patrones presentes en el texto sin formato se conservan durante el cifrado.

El CEO de Zoom, Eric S. Yuan, respondió a los hallazgos de Citizen Lab, afirmando que debido al período de alto tráfico, se vieron obligados a agregar capacidad de servidor rápidamente, y *«en nuestro apuro, agregamos por error nuestros dos centros de datos chinos a una larga lista blanca de puentes de respaldo, potencialmente permitiendo que clientes no chinos, en circunstancias extremadamente limitadas, se conecten a ellos».*

Además de todo esto, se descubrió Zoombombing, donde trolls se aprovechan de las reuniones abiertas o desprotegidas y las configuraciones predeterminadas deficientes para hacerse cargo del intercambio de pantalla y transmitir pornografía o cualquier otro material explícito. El FBI emitió una advertencia, instando a los usuarios a ajustar su configuración para evitar el secuestro de videollamadas. A partir del 4 de abril, Zoom comenzó a habilitar la

función Sala de espera (que permite al anfitrión controlar cuándo un participante se une a la reunión), y exigir a los usuarios que ingresen una contraseña para evitar abusos desenfrenados.

Zoom respondió a estas revelaciones de forma rápida y transparente, solucionando varios problemas destacados por la comunidad de seguridad cibernética.

Además, la compañía anunció un congelamiento de 90 días en el lanzamiento de nuevas funciones para *«identificar, abordar y solucionar problemas de forma proactiva»*. También tiene como objetivo realizar una revisión exhaustiva con expertos de terceros y publicar un informe de transparencia que detalle la información relacionada con las solicitudes de datos, registros o contenido de las fuerzas del orden público.

Esto ha llevado a que los usuarios dejen de confiar en la compañía. El hecho de que Zoom haya diseñado e implementado su propio cifrado es una señal de alerta, debido a que los esquemas personalizados no se someten al mismo escrutinio y revisión por pares que los estándares de cifrado que la gente utiliza hoy en día.

> *«Los problemas de seguridad más importantes con Zoom rodean características deliberadas diseñadas para reducir la fricción en las reuniones, que también, por diseño, reducen la privacidad o la seguridad»*, dijo Citizen Lab en su informe.

Citizen Lab identificó un problema grave de seguridad con la función de sala de espera de Zoom, que ha alentado a los usuarios a utilizar la función de contraseña para *«un mayor nivel de confidencialidad que las salas de espera».*

En caso de estar preocupado por Zoombombing, será necesario establecer una contraseña de reunión y bloquear una reunión cuando todos los invitados necesarios se hayan unido. Para obtener más consejos sobre cómo hacer que las llamadas de Zoom sean seguras, puedes leer la guía práctica de EFF.