Cómo reducir los riesgos en tus videoconferencias

19/04/2020

Los ciberdelincuentes siempre están buscando nuevas oportunidades para robar datos de los internautas, acceder a la información de las empresas y, a fin de cuentas, ganar dinero con todo ello. La actual situación provocada por la Covid-19 les ha abierto un abanico de posibilidades y los expertos alertan de que se está produciendo una oleada de casos de 'phishing', extorsión, 'ransomware' e intentos de brechas y violación de datos en las últimas semanas.

El aumento del teletrabajo y la necesidad de comunicarse con los seres queridos en la distancia han provocado un repunte sin precedentes en el uso de las aplicaciones de videoconferencias y esto supone un riesgo, tanto para las empresas como para los usuarios particulares. Aunque no es el único objetivo de los cibercriminales, la 'app' Zoom ha sido objeto de algunos de los incidentes más destacados en lo que va de año.

«Hay varios riesgos que hay que tener en cuenta. El primero es el de varias nuevas vulnerabilidades descubiertas en esta plataforma: una de ellas podría permitir a los hackers robar las contraseñas de Windows, y otras dos podrían permitir a los atacantes instalar remotamente malware en los Macs afectados y espiar las reuniones», advierte José Battat, director general de Trend Micro Iberia.

Los cibercriminales saben que los usuarios buscan en masa maneras de comunicarse durante los confinamientos dictados por los gobiernos. Al crear enlaces y sitios web de aspecto legítimo de Zoom -que está siendo una de las 'apps' más usadas-, podrían robar detalles financieros, propagar 'malware' o recoger números de ID de la 'app', lo que les

permitiría infiltrarse en reuniones virtuales. Un proveedor descubrió que se habían registrado 2.000 nuevos dominios solo en marzo, más de dos tercios del total del año hasta ahora.

Con tan solo el acceso a una reunión, los 'hackers' podrían recoger información corporativa altamente sensible o crítica para el mercado, e incluso propagar 'malware' a través de una función de transferencia de archivos. Estos problemas a nivel empresarial también pueden afectar a los usuarios particulares, ya sea mediante robo de datos personales o accediendo a las reuniones (en ocasiones entre menores) para publicar comentarios ofensivos o transmitir contenido inapropiado, por ejemplo.

Consejos de los expertos
Desde Trend Micro ofrecen una serie de recomendaciones de seguridad, que parten de cuestiones sencillas, como es el hecho de tener las aplicaciones siempre actualizadas a la última versión o «asegurarse de que todos los teletrabajadores -en el caso de las empresas- tengan un programa 'antimalware', incluida la detección de 'phishing' instalada de un proveedor de confianza».

¿Cómo mantienes tus piernas cuando estás sentado y qué te dice tu postura sentada?
A continuación, es importante revisar los ajustes de administración de la aplicación, para reducir las oportunidades de los cibercriminales. En este punto, puede ser interesante establecer una contraseña para la reunión y optar por que solo puedan participar los usuarios que han sido previamente registrados. Esos links que se crean para la reunión, junto a la identificación de los usuarios, son la puerta de entrada de los 'hackers'.

«También recomendamos asegurarse de que se genera un ID de reunión automáticamente para las reuniones recurrentes;

configurar la pantalla compartida como ‘solo host’ para evitar que los asistentes no invitados compartan contenido perjudicial; o desactivar las ‘transferencias de archivos’ para mitigar el riesgo de malware», detalla José Battat.

Aplicaciones como Zoom también permiten activar un sonido cada vez que alguien entra o sale de la reunión, de forma que podamos detectar la entrada de ‘intrusos’ o, incluso, bloquear la reunión una vez que haya empezado para evitar que alguien se una a ella. Una serie de trucos que pueden ayudar a los usuarios a garantizar una comunicación segura.

Herramientas gratuitas

Algunos proveedores de soluciones de ciberseguridad están ofreciendo algunos de sus productos o servicios de forma gratuita durante la crisis del Covid-19. Es el caso de Trend Micro, que comparte algunos recursos que puede ayudar a trabajar y navegar por la Red de manera más segura durante este tiempo.

Así, cualquier usuario puede descargar seis meses gratis de Trend Micro Maximum Security, un producto de seguridad para uso doméstico en ordenadores Windows o Mac, así como la versión móvil, con una prueba gratuita de seguridad máxima de un mes a la que se puede acceder desde la tienda de aplicaciones del ‘smartphone’.

Esta compañía también ha habilitado otras herramientas y servicios gratuitos para empresas, como licencias temporales gratuitas por 60 días de Worry-Free Services; simulaciones de phishing para mantener seguros a trabajadores remotos con Phish Insight; Cloud App Security, para proteger Office365/GoogleApps; Deep Security, para proteger los servidores; y Web Security, para garantizar la seguridad de la navegación