Microsoft parcheó una vulnerabilidad similar a un gusano en su plataforma de chat y vudeo en el lugar de trabajo de Teams, que podría haber permitido a los hackers tomar el control de toda la lista de cuentas de Teams de una organización simplemente enviando a los participantes un enlace malicioso a una imagen que parece inocente.

Los investigadores de seguridad cibernética de CyberArk descubrieron la vulnerabilidad, que afecta a las versiones de escritorio y web de la aplicación. Luego de que los hallazgos se divulgaron de forma responsable el 23 de marzo, Microsoft parchó la vulnerabilidad en una actualización publicada el 20 de abril.

> *«Incluso si un atacante no reúne mucha información de la cuenta de un equipo, aún podría usar la cuenta para recorrer toda la organización (como un gusano)»,* dijo Omer Tsarfati de CyberArk.
>
> *«Eventualmente, el atacante podría acceder a todos los datos de las cuentas de los equipos de su organización, recopilar información confidencial, información de reuniones y calendario, datos competitivos, secretos, contraseñas, información privada, planes de negocios, etcétera».*

El desarrollo se produce cuando el software de videoconferencia como Zoom o Microsoft Temas, están presenciando un aumento sin precedentes en la demanda, ya que las empresas, los estudiantes e incluso los empleados del gobierno de todo el mundo se ven obligados a trabajar y socializar desde su hogar durante la pandemia del coronavirus.

La vulnerabilidad se debe a la forma en que Microsoft Teams maneja la autenticación de los recursos de imagen. Cada vez que se abre la aplicación, se crea un token de acceso, un token web JSON (JWT) durante el proceso, lo que permite que el usuario pueda ver imágenes compartidas por otras personas en una conversación.

Los investigadores de CyberArk descubrieron que podían obtener una cookie llamada *«authoken»*, que otorga acceso a un servidor de recursos (api.spaces.skype.com), y la usaron para crear el *«token de skype»* mencionado anteriormente, con lo que se logra obtener permisos ilimitados para enviar mensajes, leer mensajes, crear grupos, agregar nuevos usuarios o eliminar usuarios de grupos y cambiar permisos en grupos por medio de la API de Teams.

Debido a que la cookie authoken está configurada para enviarse a teams.microsoft.team o cualquiera de sus subdominios, los investigadores descubrieron dos subdominios (aadsync-test.teams.microsoft.com y data-dev.teams.microsoft.com), que eran vulnerables a los ataques de toma de control.

> *«Si un atacante de alguna forma puede obligar a un usuario a visitar los subdominios de los que se han apoderado, el navegador de la víctima enviará esta cookie al servidor del atacante, y el atacante (después de recibir el token automático), puede crear un token de Skype. Después de hacer todo esto, el atacante puede robar los datos de la cuenta del equipo de la víctima»,* agregaron los investigadores.

Una vez con los subdominios comprometidos, un hacker podría explotar la vulnerabilidad simplemente enviando un enlace malicioso, como un GIF, a una víctima desprevenida o a todos los miembros de un chat grupal. Por lo tanto, cuando los destinatarios abren el mensaje, el navegador intenta cargar la imagen, pero no antes de enviar las cookies autorizadas al subdominio comprometido.

El atacante puede utilizar la cookie de autenticación automática para crear un token de Skype y, por lo tanto, acceder a los datos de la víctima. Lo que es peor, el ataque puede ser montado por cualquier extraño, siempre que la interacción implique una interfaz de chat, como una invitación a una llamada de conferencia para una posible entrevista de trabajo.

> *«La víctima nunca sabrá que ha sido atacada, lo que hace que la explotación de esta vulnerabilidad sea sigilosa y peligrosa»,* dijeron los investigadores.

## Ataques a plataformas de videoconferencia en aumento

El cambio al trabajo en casa debido a la pandemia por el COVID-19, ha hecho que la demanda de servicios de videoconferencia crezca demasiado, convirtiéndose en una oportunidad para que los hackers roben credenciales y distribuyan malware.

Investigaciones recientes de Proofpoint and Abnormal Security, descubrieron campañas de ingeniería social que solicitan a los usuarios unirse a una reunión de Zoom o abordar una vulnerabilidad de seguridad de Cisco WebEx haciendo clic en enlaces maliciosos diseñados para robar credenciales de inicio de sesión.

Ante dichas amenazas emergentes, se recomienda a los usuarios que estén atentos a correos electrónicos de fuentes no confiables y mantengan su software de videoconferencia actualizado.