Investigadores de seguridad cibernética revelaron este fin de semana algunos detalles sobre nuevos riesgos de seguridad asociados con las vistas previas de enlaces en aplicaciones de mensajería populares, que hacen que los servicios filtren direcciones IP, expongan enlaces enviados a través de chats cifrados de extremo a extremo e incluso descarguen de forma innecesaria GB de datos de forma sigilosa en segundo plano.

> *«Los enlaces compartidos en los chats pueden contener información privada destinada únicamente a los destinatarios»*, dijeron los investigadores Talal Haj Bakry y Tommy Mysk.
>
> *«Pueden ser facturas, contratos, registros médicos o cualquier cosa que pueda ser confidencial. Las aplicaciones que dependen de los servidores para generar vistas previas de enlaces pueden violar la privacidad de sus usuarios al enviar enlaces compartidos en un chat privado a sus servidores»,* agregaron los investigadores.

Las vistas previas de enlaces son una característica común en la mayoría de las aplicaciones de chat, que facilita la visualización de una vista previa incluyendo una breve descripción del enlace compartido.

Aunque aplicaciones como Signal y Wire brindan a los usuarios la opción de activar/desactivar las vistas previas de enlaces, algunas otras como Threema, TikTok y WeChat no generan una vista previa de enlaces en absoluto.

Las aplicaciones que generan vistas previas lo hacen al final del remitente o del destinatario o mediante un servidor externo que luego se envía de regreso tanto al remitente como al destinatario.

Las vistas previas de enlaces del lado del remitente, utilizadas en Apple iMessage, Signal (al tener activada la configuración), Viber y WhatsApp de Facebook, funcionan al descargar el enlace, seguido de la extracción de la imagen de vista previa y el resumen, que luego se

envía al destinatario como un archivo adjunto. Cuando la aplicación en el otro extremo recibe la vista previa, muestra el mensaje sin abrir el enlace, protegiendo así al usuario de enlaces maliciosos.

> *«Este enfoque asume que quien envía el enlace debe confiar en él, ya que será la aplicación del remitente la que tendrá que abrir el enlace»,* dijeron los investigadores.

Por el contrario, las vistas previas de enlaces generadas en el lado del destinatario abren la puerta a nuevos riesgos que permiten a un mal actor medir su ubicación aproximada sin que el receptor realice ninguna acción simplemente al enviar un enlace a un servidor bajo su control.

Esto se debe a que la aplicación de mensajería, al recibir un mensaje con un enlace, abre la URL automáticamente para crear la vista previa al revelar la dirección IP del teléfono en la solicitud enviada al servidor.

Se descubrió que Reddit Chat y una aplicación no revelada, que está en *«proceso de solucionar el problema»,* siguen este enfoque, según los investigadores.

Finalmente, el uso de un servidor externo para generar vistas previas, al tiempo que evita el problema de fuga de direcciones IP, crea más problemas, como que el servidor podría retener una copia, y de ser así, surge la interrogante de cuánto tiempo la almacena y para qué la utilizan.

Algunas aplicaciones, entre ellas Discord, Facebook Messenger, Google Hangouts, Instagram, Line, LinkedIn, Slack, Twitter y Zoom, entran en esta categoría, sin ninguna indicación para los usuarios de que *«los servidores están descargando lo que encuentran en un enlace».*

La prueba de estas aplicaciones reveló que, a excepción de Facebook Messenger e Instagram, todas las demás impusieron un límite de 15 a 50 MB cuando se trata de los archivos descargados por sus respectivos servidores. Slack, por ejemplo, almacena en caché las vistas previas de enlaces durante unos 30 minutos.

Facebook Messenger e Instagram descargaron archivos completos, incluso si tenían un tamaño de gigabytes, que según Facebook, es una característica prevista.

Entonces, los investigadores advierten que esto podría ser una *«pesadilla de privacidad»* si los servidores retienen una copia y *«alguna vez hay una violación de datos de estos servidores».*

A pesar de la función de cifrado de extremo a extremo de Line (E2EE) diseñada para evitar que terceros escuchen las conversaciones, la dependencia de la aplicación en un servidor externo para generar vistas previas de enlaces permite que *«los servidores de Line conozcan todo acerca de los enlaces que se envían a través de la aplicación y quién comparte qué enlaces a quién».*

Desde entonces, LINK ha actualizado sus preguntas frecuentes para especificar que *«para generar vistas previas de URL, los enlaces compartidos en los chats también se envían a los servidores de LINE».*

En otro caso, los investigadores también descubrieron que era posible ejecutar código malicioso en servidores de vista previa de enlaces, lo que resultaba en un enlace de código JavaScript compartido en Instagram o LinkedIn para hacer que sus servidores ejecutaran el código.

> *«Probamos esto enviando un enlace a un sitio web en nuestro servidor que contenía código JavaScript que simplemente hizo una devolución de llamada a nuestro servidor. Pudimos confirmar que teníamos al menos 20 segundos de tiempo de ejecución en estos servidores»,* dijeron los investigadores.

Bakry y Mysk expusieron previamente fallas en TikTok, que hicieron posible que los atacantes mostraran videos falsificados, incluidos los de cuentas verificadas, al redirigir la aplicación a un servidor falso que aloja una colección de videos falsificados.

A inicios de marzo, los investigadores también descubrieron un problema de privacidad considerable por parte de más de 4 docenas de aplicaciones de iOS que se encontraron para acceder a los portapapeles de los usuarios sin su permiso explícito.

> *«Las vistas previas de enlaces son una buena característica de la que los usuarios generalmente se benefician, pero aquí hemos demostrado la amplia gama de problemas que esta característica puede tener cuando las preocupaciones de privacidad y seguridad no se consideran cuidadosamente».*