Nuevos descubrimientos han arrojado luz sobre lo que se describe como un intento legal de secretamente interceptar el tráfico que proviene de jabber[.]ru (también conocido como xmpp[.]ru), un servicio de mensajería instantánea basado en XMPP, a través de servidores alojados en Hetzner y Linode (una filial de Akamai) en Alemania.

> *«El agresor ha emitido varios certificados TLS recientes utilizando el servicio Let's Encrypt que fueron empleados para tomar el control de conexiones STARTTLS encriptadas en el puerto 5222 utilizando un proxy transparente de [hombre en el medio]»*, expresó un investigador de seguridad que utiliza el alias ValdikSS a principios de esta semana.

> *«Se descubrió el ataque debido al vencimiento de uno de los certificados MiTM, que no se renovaron».*

Las pruebas recopiladas hasta el momento indican que la redirección del tráfico está configurada en la red del proveedor de alojamiento, descartando otras posibilidades, como una violación del servidor o un ataque de suplantación.

Se estima que la interceptación ha tenido lugar durante un período de hasta seis meses, desde el 18 de abril hasta el 19 de octubre, aunque se ha confirmado que ocurrió al menos desde el 21 de julio de 2023 hasta el 19 de octubre de 2023.

Los indicios de actividad sospechosa se detectaron por primera vez el 16 de octubre de 2023, cuando uno de los administradores UNIX del servicio recibió un mensaje que decía «El certificado ha caducado» al conectarse al mismo.

Se cree que el actor de amenazas detuvo la actividad después de que comenzara la investigación sobre el incidente de MiTM el 18 de octubre de 2023. No está claro de inmediato quién está detrás del ataque, pero se sospecha que se trata de una interceptación

legal basada en una solicitud de la policía alemana.

Otra teoría, aunque poco probable pero no imposible, es que el ataque de MiTM sea una intrusión en las redes internas de tanto Hetzner como Linode, concretamente apuntando a jabber[.]ru.

> *«Dada la naturaleza de la interceptación, los agresores han tenido la capacidad de llevar a cabo cualquier acción como si se realizara desde la cuenta autorizada, sin necesidad de conocer la contraseña de la cuenta»,* indicó el investigador.

> *«Esto implica que el agresor podría descargar la lista de contactos de la cuenta, acceder al historial de mensajes en el servidor sin cifrar, enviar mensajes nuevos o modificarlos en tiempo real».*

Se recomienda a los usuarios del servicio que asuman que sus comunicaciones de los últimos 90 días están comprometidas, además de *«verificar sus cuentas en busca de nuevas claves OMEMO y PGP no autorizadas en su almacenamiento PEP, y cambiar sus contraseñas».*