Publicado en Madrid el 13/07/2022

Los ciberdelincuentes acentúan sus esfuerzos en las redes sociales profesionales

La empresa española S2 Grupo, especializada en ciberseguridad así como ciberinteligencia y gestión de sistemas críticos, advierte de que cada vez es mayor la actuación de los ciberdelincuentes en redes sociales, como por ejemplo Linkedini, lo que pone en situación de vulnerabilidad a las personas y los entornos en los que trabajan

Según ha informado la compañía en un comunicado, los grupos organizados de ciberdelincuencia internacional actúan a través de este tipo de redes sociales con el propósito de obtener dinero o datos a través del ciberespionaje. “El objetivo de los cibercriminales siempre es el mismo, obtener dinero u obtener datos, porque la información vale mucho dinero. Muchas personas creen que los casos de phising sólo se pueden dar a través de un email que suplanta identidad y de enlaces maliciosos, pero esto no es así. Esto se ha sofisticado y también nos encontramos con casos de phising en LinkedIn, por ejemplo”, ha explicado José Rosell, socio-director de S2 Grupo.

“Existen grupos de ciberdelincuencia como el coreano Lazarus que, precisamente, hacen un uso intensivo de redes como LinkedIn para generar un primer contacto con sus víctimas. Esto requiere que extrememos las precauciones en el uso de estas redes sociales para evitar caer en su trampa, muchas veces orientada hacia el ciberespcionaje”, ha afirmado Miguel A. Juan, socio-director de S2 Grupo.

El equipo de expertos de la compañía de ciberseguridad ha destacado que el modus operandi de estos grupos de cibercrimen suele comenzar con un estudio del perfil objetivo. Es decir, los cibercriminales analizan a la víctima para acercarse a ella “sin crear sospechas”. De esta forma, estudian sus intereses, su entorno, contactos, la empresa a la que pertenecen, etc. pasando desapercibidos

El segundo paso para este tipo de ataques, es realizar una aproximación a medida. Con la víctima estudiada, se envía algún mensaje o se realiza un contacto inicial a medida. "Por ejemplo, si mis intereses son X o mi trabajo es Y, en función de mi perfil, el acercamiento será adecuado a ese trabajo, intereses, perfil, etc. Esto incrementará las probabilidades de éxito”, ha asegurado José Rosell.

En tercer lugar, es clave la confianza. Los grupos de ciberdelincuentes inician un intercambio de mensajes que parecen inocuos para ganarse la confianza de la víctima.

Por último, llega lo que los expertos de S2 Grupo denominan como “delivery”. Una vez establecido el contacto, habiendo cierta confianza y seguridad en la conversación, aprovechan para realizar el envío de un código dañino. Este mensaje puede incluir adjuntos o enlaces que permitirán al ciberdelincuente el control total (por ejemplo, mediante despliegue de un RAT, software capaz de realizar tareas de espionaje y monitoreo del equipo infectado) o parcial (por ejemplo, mediante la captura de credenciales válidas) de su víctima.

Datos de contacto:
Luis Núñez
667574131

Nota de prensa publicada en: Madrid

Categorías: Nacional E-Commerce Ciberseguridad