LinkedIn, portal favorito de cibercriminales para estafar

¿Qué es LinkedIn?

LinkedIn es la red profesional más grande del mundo en Internet. Esta web conecta a empresas y empleados, en ella puedes encontrar el trabajo o la pasantía adecuada para ti. Además, puedes fortalecer tus relaciones profesionales y aprender las habilidades que necesitas para tener éxito en tu carrera

Sin embargo, la aplicación se está convirtiendo en el lugar donde ocurren con frecuencia estafas y robos de datos.

Ya han sido varias las compañías de ciberseguridad que han advertido sobre los peligros a los que se exponen los usuarios de **LinkedIn** si no mantienen cautela con su información personal y lo que publican en sus perfiles. Esto porque la plataforma desde hace ya un tiempo **se ha convertido en uno de los sitios favoritos de los cibercriminales para estafar personas y robar datos.**

José Rosell, director de S2 Grupo, explica que "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 solo 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".

La compañía también relata que son varios los grupos de ciberdelincuencia que hacen uso de la conocida plataforma de relacionamiento profesional para acercarse por primera vez a sus potenciales víctimas, por ejemplo, el conocido **Lazarus es**

una de estas organizaciones criminales que suelen "lanzar sus carnadas en LinkedIn". Además no solo se busca estafar y robar los datos de los usuarios, sino que también se han llevado a cabo campañas de ciberespionaje en la red social.
Estos son los 4 pasos que usan los atacantes:

1, Observar el objetivo

Como primer paso, los criminales cibernéticos se hacen una idea de los usuarios a los que planean atacar, **estudiando su perfil y comportamiento en la red,** la información que mantienen pública, el contenido que comparten, los contactos con los que interactúan y a lo que le dan like o reaccionan.

2. Primer acercamiento

Habiendo "stalkeado" a la persona, ahora diseñarán la mejor manera de contactarse con ella por primera vez, probablemente **buscarán un "pretexto" relacionado con los intereses de la potencial víctima** para asegurarse de que el acercamiento resulte exitoso para ellos.

3. Ganarse la confianza

Este es el momento en el que más se esfuerzan los delincuentes, pues tienen que mantener la atención de los usuarios en la conversación que han iniciado con ellos, además tienen que ganarse su confianza. Es por ello que usualmente **toman la imagen de una entidad legítima o se hacen pasar por organización muy profesional que ofrece distintos tipos de servicios como cursos,** aunque en realidad esa empresa no exista.

4. "La estocada final en LinkedIn"

Infobae ha definido el último paso con este nombre, la empresa de ciberseguridad lo ha denominado "Delivery", pero a la final

describen lo mismo, pues **es el momento en que los criminales cibernéticos por fín hacen su ataque y ya no hay nada que la víctima pueda hacer.**

Ya la contactaron, le enviaron un mensaje con una presunta oferta muy interesante en nombre de una empresa fidedigna, incluso mantuvieron conversaciones con ella y **ahora que se ganaron su confianza, le envían un link invitando a que lo abra ya que contiene información importante.**

Una vez se haya abierto este enlace enviado por los ciberdelincuentes existen dos posibilidades de ataque, por un lado **puede ser el típico formulario para rellenar con datos personales,** de esta manera los criminales se quedarán con información valiosa que pueden utilizar **para extorsionar a la persona más adelante.**

Pero el escenario más desafortunado es si este hipervínculo resulta siendo un **malware oculto** también denominado como RAT, que es un **software capaz de tomar control total sobre el computador y realizar actividades de espionaje y monitoreo del sistema.**