



Los ciberdelincuentes explotan la logística como anzuelo para propagar ‘malware’

El brote de coronavirus ha provocado un aumento de las estafas o ‘phishing’ ligados al sector logístico. Este tipo de ataques utilizan correos electrónicos con cuestiones ligadas al comercio o la logística, como pedidos y reservas, para dirigirse a las organizaciones y propagar malware a través de archivos adjuntos. Así lo ha alertado la compañía de ciberseguridad Kaspersky, que ha asegurado que estos ataques son especialmente peligrosos para “empleados de las organizaciones que venden mercancías”, debido a que a menudo reciben solicitudes de suministros y diversos pedidos.

Según esta empresa, “puede resultar complicado determinar si un correo electrónico es real o no, incluso para empleados atentos, por lo que el número de estafas están en aumento”. En los casos más recientes, Kaspersky ha explicado que los ciberdelincuentes se han referido a “problemas de entrega derivados de la

pandemia”. En concreto, estas estafas pueden indicar que un proveedor en China no puede producir los productos a tiempo para comprobar si la víctima puede facilitar la información necesaria para cumplir el pedido. En algunos casos, los ciberdelincuentes incluso hacen referencia a pedidos urgentes y “esto supone una presión adicional para las víctimas”, ha señalado la compañía especializada en ciberataques.

El objetivo principal de estos correos electrónicos es lograr que la víctima abra un archivo adjunto malicioso que infecta el dispositivo y entregue así a los ciberdelincuentes el control remoto o el acceso al sistema de la organización. Con el fin de provocar esta apertura, los infractores piden a las víctimas que comprueben la información de entrega, pago o detalles del pedido que aparentemente se encuentran en el archivo adjunto.

Por ello, la mejor medicina contra este tipo de amenazas es “una buena solución de seguridad que pueda detectar diversas amenazas en los archivos adjuntos y que cuente con una base de datos de catalogación de este tipo de estafas”, ha recomendado la analista principal de contenidos web de Kaspersky, Tatyana Shcherbakova. El otro consejo es “mantener la calma y estar atento a los detalles, y esto es algo que debemos seguir haciendo independientemente de cualquier circunstancia externa», ha añadido.