El coronavirus genera la mayor oleada de ciberataques por email en años

EFE | El uso del Covid-19 como cebo ha generado un volumen de ataques por correo electrónico que «representa la mayor colección de tipos de ciberataque» registrados bajos un mismo tema en «años o incluso en la historia», según la empresa de ciberseguridad *Proofpoint*.

La empresa constata el uso del coronavirus como gancho en envíos de *phishing* de credenciales, ficheros adjuntos, enlaces y programas maliciosos o correo basura, entre otras amenazas.

Durante más de cinco semanas, se observa «numerosas campañas de correo malicioso ligadas al Covid-19, muchas de ellas utilizando el miedo para convencer a las víctimas de que hagan clic», indica n.

El uso de Covid-19 como cebo «es una campaña de ingeniería social a gran escala

-advierte-. Los atacantes saben que la gente está buscando información segura y que está más predispuesta a hacer clic en cualquier enlace o a descargar archivos adjuntos».

Aproximadamente el 70% de los correos que ha descubierto el equipo de amenazas de Proofpoint contiene malware (programa malicioso), y casi un 30% tiene como objetivo robar datos de credenciales de las víctimas, señala la nota.

La mayoría de estos correos pretenden robar credenciales utilizando falsas webs de acceso a Gmail o a Office 365, pidiendo a las personas que introduzcan su nombre de usuario y su contraseña.

«Los criminales han enviado oleadas de correos que han variado desde varias docenas hasta más de 200 000 al mismo tiempo»; el número de campañas continúa aumentando y se detectan entre tres y cuatro cada día en todo el mundo.

Los expertos registran además nuevos ataques de «prolíficos grupos de hackers» que ponen en marcha sofisticadas campañas dirigidas a las industrias farmacéuticas, de salud y manufacturera de Estados Unidos, así como a servicios públicos, indica el comunicado.

Se destacan, entre otros ejemplos, un malware desconocido denominado RedLine Stealer, que aprovecha la predisposición de la gente a ayudar a encontrar una cura para el Covid-19 a través de un proyecto informático distribuido para investigación de enfermedades.

Además detectan correos dirigidos a padres y cuidadores con un *malware* llamado Ursnif que puede robar información como la de cuentas bancarias y otros encaminados a organizaciones de salud, ofreciendo remedios para el coronavirus a cambio de bitcoins.

Otros correos incluyen falsas guías sobre cómo proteger del coronavirus a familia y amigos, que invitan a los usuarios a clicar en enlaces maliciosos.