21sec advierte sobre el ransomware Emotet

Emotet se ha presentado como un nuevo riesgo para corporativos y oficinas de gobierno del mundo, de acuerdo con **S21sec, compañía española de seguridad informática**, que ha reportado en un comunicado el descubrimiento de una nueva amenaza de ransomware. Este ataque se lleva a cabo mediante una campaña de spam que propaga un virus troyano en sistemas operativos **Windows**.

Emotet se propaga a través de una red de correos fraudulentos. Las víctimas **reciben un correo electrónico con un enlace que descarga un documento en formato Word**; al abrir el archivo en la computadora, se muestra una leyenda que indica que es un archivo protegido, y que se deben habilitar las macros para poder visualizarlo. La macro en cuestión se encarga de descargar y ejecutar el malware.

Emotet, una vez instalado en el sistema operativo, roba información personal incluyendo las credenciales bancarias del usuario. Después ejecuta su protocolo de propagación, ya sea a través del correo electrónico de la víctima, o de una red interna empresarial.

Se han identificado varios enlaces con urls dentro de los siguientes dominios: auksteja.lt ; avantif.maindev.fr ; christythematchmaker.com; cypersinger.com; purpleinc.in.

S21sec recomienda no abrir enlaces que estén en correos electrónicos marcados como SPAM o que provengan de un remitente desconocido. También es importante involucrar a toda la organización en una cultura de seguridad digital, ya que si un usuario es vulnerado, este pondrá en riesgo a toda la red.