# ransomware

# REvil

# ¿Qué tipo de amenaza es?

Es un ransomware, es decir, es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos.

# ¿Cómo comienza y cómo se propaga esta amenaza?

El ransomware REvil, también conocido como Sodinokibi, afectó a más de 1.000 compañías en al menos 17 países del mundo mediante un ataque de cadena de suministro utilizando un instalador de una actualización automática del software de gestión de IT de la compañía Kaseya, que es utilizado comúnmente por proveedores de servicios administrados.

La actualización con permisos de administrador afectó a los MSP y estos a su vez infectaron los sistemas de sus clientes con la amenaza.

# ¿Hay más de una amenaza aplicada?

En este caso no, este ransomware actuó solo, encriptando todos los archivos (sin robarlos) y pedir dinero a cambio de restaurarlos.

# ¿Qué solución o medida recomendarían?

Por su parte, la Agencia Nacional de Ciberseguridad de Estados Unidos junto al FBI publicaron una guía para los proveedor de servicios administrados afectados por este ataque así como para sus clientes, que incluye, entre otros puntos, descargar la herramienta de detección de Kaseya VSA, la cual analiza un sistema e indica si se detecta la presencia de algún Indicador de compromiso.

Mientras que la Kaseya notificó a las personas potencialmente afectadas con la recomendación de cerrar posibles servidores VSA de manera inmediata hasta tanto se publique el parche.