

# Clase 24: Amenazas

# TIPO DE AMENAZA

RAMSOMWARE: El malware de rescate, o ransomware, 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 como se propaga?

Normalmente, su primera acción la realiza a través de un ataque de phishing en este caso basado en **Emotec**, un troyano que cambia su código cada poco tiempo a fin de no ser detectado por las soluciones de seguridad y que tiene la capacidad de interceptar, registrar, y guardar todo el tráfico de red.

## ¿Hay más de una amenaza aplicada?

Si, funcionan tres amenazas distintas. Una vez que Emotec ha realizado su trabajo, empieza el turno de Trickbot, que se encarga de los ataques laterales, entre otros, el robo de las credenciales de inicio de sesión. Una vez que ambos malware han acabado con su labor, Ryuk es el encargado de encriptar todos los datos.

## ¿Qué solución o medida recomendarían?

- Mantener actualizado los backup para restaurar al punto de ese backup.
- Hacer una copia de seguridad en un disco externo.
- Mantener un sistema de seguridad adaptable a un entorno cambiante.