● ¿Qué tipo de amenaza es?
Ransomware Ryuk. Ryuk es uno de los ransomware que más estragos está causando en la actualidad.

● ¿Cómo comienza y cómo se propaga esta amenaza?
Se propaga a través del correo electrónico con suplantación de identidad, en el cual se utiliza software de explotación como Fiesta o Magnitud para tomar el control del sistema, cifrar archivos y así pedir el pago del rescate del computador.

● ¿Hay más de una amenaza aplicada?
Ryuk no trabaja sólo: necesita la ayuda de otros virus para poder ejecutarse. Normalmente, su primera acción la realiza a través de un ataque de phishing 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.
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?
Prevención:
- Nunca haga clic en enlaces peligrosos.
- Evite revelar información personal.
- No abra archivos adjuntos de correos electrónicos sospechosos.
- No utilice nunca memorias USB desconocidas.
- Mantenga sus programas y sistema operativo actualizados.
- Utilice solo fuentes de descarga conocidas.
- Utilice servicios VPN en las redes Wi-Fi públicas.

Una vez infectado:
- Crear una copia del disco duro comprometido para tratar de recuperar los datos sobre el clon.
- Desinfectar la copia.
- Conservar el disco duro cifrado si no se pudo descifrar.