¿Qué tipo de amenaza es?

Es un Ransomware (Ryuk)

¿Cómo comienza y cómo se propaga esta amenaza?

Arranca con 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.

¿Hay más de una amenaza aplicada?

Si,

¿Qué solución o medida recomendarían?

Si, lo mejor sería aumentar el presupuesto en ciberseguridad y reducir el tiempo de reacción contra las amenazas. Adquirir defensas dinámicas ya que el entorno es cada vez más cambiante.