**Actividad**

https://revistabyte.es/ciberseguridad/ryuk-ministerio-de-trabajo/

● ¿Qué tipo de amenaza es?

Ryuk es uno de los ransomware que más estragos está causando en la actualidad, es el preferido de los ciberdelincuentes para atacar a Administraciones Públicas

● ¿Cómo comienza y cómo se propaga esta amenaza?

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. La gravedad de éste radica en su capacidad de infección y es que, no sólo encripta los equipos sino también la práctica totalidad de los recursos de la red.

● ¿Hay más de una amenaza aplicada?

No

● ¿Qué solución o medida recomendarían?

Se hace imposible la restauración del sistema ya que desabilita esa opción en Windows, por lo que solo mediante el pago a los ciberdelicuentes permitiría la desencriptación de los datos.