Mesa 1

Nota : <Ryuk: el ransomware que atacó al Ministerio de Trabajo (revistabyte.es)>

¿Qué tipo de amenaza es?

Ransomware Restringen el acceso a su sistema y archivos.

¿Cómo comienza y cómo se propaga esta amenaza?

A través de correos de phishing con archivos adjuntos o enlaces. Mediante ataques a conexiones remotas, como el Protocolo de Escritorio Remoto (RDP), aprovechando el uso de contraseñas débiles. También a través de la explotación vulnerabilidades por ejemplo, mediante sitios web comprometidos utilizados para redirigir a sus visitantes a diferentes tipos de exploits—, así como también dispositivos USB, descarga de software pirata, entre otros.

¿Hay más de una amenaza aplicada ?

Su principal característica es que 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.

¿Qué solución o medida recomendarían ?

En primer instancia, recomendaríamos apagar la computadora y desconectarla de la red. Identificar la amenaza, si es posible; utilizar una herramienta específica para recuperar el acceso a los archivos.

Finalmente, antes de pagar el rescate, recomendamos recuperar la información a través de un backup -que siempre se debe tener debido a la importancia de la información- y por otro lado recomendamos al Ministerio de Trabajo presupuesto en cirberseguridad.