Clase 24 - Mauricio Ortiz Henao

¿Qué tipo de amenaza es?

Ransomware

¿Cómo comienza y cómo se propaga esta amenaza?

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.

¿Hay más de una amenaza aplicada?

Malwares con nombres Emotec, Trickbot

¿Qué solución o medida recomendarían?

Se debería aumentar el presupuesto en ciberseguridad porque no es un problema de voluntad de los CISOs sino de presupuesto y del tiempo de reacción contra las amenazas.

En muchas ocasiones, se creen que con defensas estáticas pueden defenderse y hay que adaptarse a un entorno cada vez más cambiante y que tiene nuevas técnicas de ataque cada menos tiempo.