Clase 24 – Amenazas

El ransomware **Ryuk** .

Normalmente desde que el malware empieza a infectar, hasta que se descubre la incidencia o se bloquean los equipos transcurren **alrededor de varios meses**,

Es un virus que entra por un correo (phisihing) 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.

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

Guarda el tráfico de red, robo de credenciales de inicios de sesión y encriptación los datos de sistema.

2) Conclusión: se debería aumentar el presupuesto en ciberseguridad.