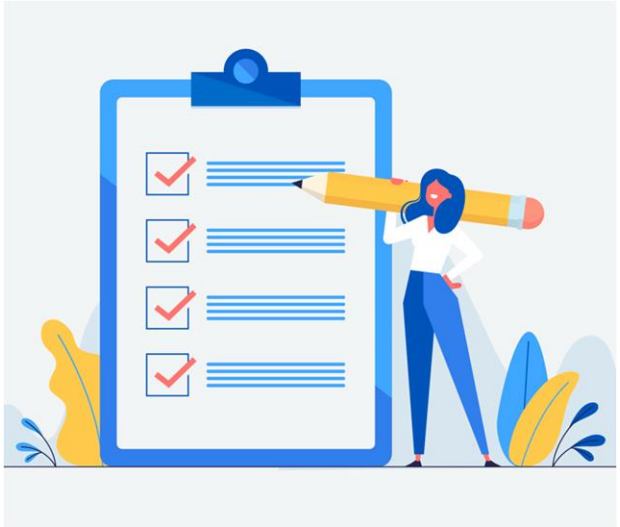
Actividad Tipos de Amenazas

Utilizando este documento de presentación, cada mesa deberá resolver y completar en cada hoja , que le corresponde según su número de mesa.



Mesa 7

Nota: <Ataque masivo del ransomware REvil comprometió más de 1000 compañías en mundo | WeLiveSecurity>

¿Qué tipo de amenaza es?

Ransomware
Es un malware o código malicioso que tiene como objetivo cifrar los datos de la computadora de la víctima impidiendo el acceso y solicitando un pago de “rescate generalmente en bitcoins.

¿Cómo comienza y cómo se propaga esta amenaza?

Comenzó por la actualización con permisos de administrador que afectó a los MSP y estos a su vez infectaron los sistemas de sus clientes con la amenaza; fue un ataque de cadena de suministro utilizando un instalador de una actualización automática del software de gestión de IT de la compañía Kaseya.

¿Hay más de una amenaza aplicada?

No, en este caso particular no se robó la información previamente a la encriptación, algo que es una práctica común en este tipo de ataques.

Mesa 7

Nota: <Ataque masivo del ransomware REvil comprometió más de 1000 compañías en mundo | WeLiveSecurity>

¿Qué solución o medida recomendarían?

1. Se recomienda que aquellas empresas que tienen servidores que pueden haber sido comprometidos por este ataque que se mantengan informadas y que apaguen las máquinas potencialmente vulnerables o que al menos las aíslen de la red hasta que aparezca más información, mencionaron Goretsky y Camp.
2. Por su parte, la Agencia Nacional de Ciberseguridad de Estados Unidos junto al FBI publicaron una guía para los proveedor de servicios administrados afectados por este ataque así como para sus clientes, que incluye, entre otros puntos, descargar la herramienta de detección de Kaseya VSA, la cual analiza un sistema e indica si se detecta la presencia de algún Indicador de compromiso.