Práctica integradora

Objetivo

Vamos a poner en práctica los conocimientos que hemos adquirido hasta el momento. Se crearán grupos, divididos en sus respectivas salas y realizarán la siguiente ejercitación.

Ataque masivo del ransomware REvil comprometió más de 1000 compañías en mundo.

- **¿Qué tipo de amenaza es?**

  Ransomware REvil

- **¿Cómo comienza y cómo se propaga esta amenaza?**

  Atacaron a los servidores de Kaseya VSA a través de la explotación de una vulnerabilidad zero-day que estaba en proceso de ser reparada, enviando el ransomware REvil afectando a más de 1000 compañías y comprometiendo a más de 1 millón de sistemas.

  El mismo se propaga a través del correo electrónico con suplantación de identidad, en el cual se utiliza software de explotación como Fiesta o Magnitud para tomar el control del sistema, cifrar archivos y así pedir el pago del rescate del computador.

  El ransomware puede infectar su ordenador de varias formas. Uno de los métodos más habituales actualmente es a través de spam malicioso, o malspam, que son mensajes no solicitados que se utilizan para enviar malware por correo electrónico.

El pago solicitado a cada víctima de este ataque fue distinto para cada caso, llegando a 5 millones de dólares el monto más elevado que algunos investigadores aseguran haber visto.

- **¿Hay más de una amenaza aplicada?**

  Sí, En este caso, el ataque masivo del ransomware REvil, también conocido como Sodinokibi, afectó a más de 1.000 compañías en al menos 17 países del mundo mediante un ataque de cadena de suministro utilizando un instalador de una actualización automática del software de gestión de IT de la compañía Kaseya, que es utilizado comúnmente por proveedores de servicios administrados.

  La actualización con permisos de administrador afectó a los MSP y estos a su vez infectan los sistemas de sus clientes con la amenaza, como fue el caso de una cadena de supermercados en Suecia que tuvo que cerrar algunas tiendas y al menos 11 escuelas en Nueva Zelanda.

- **¿Qué solución o medida recomendarían?**

  Según lo comentado en el artículo, podríamos recomendar dos grandes medidas, utilizar la herramienta de detección de Kaseya VSA para analizar el sistema e indica si se detecta la presencia de algún Indicador de compromiso y en función de eso, formatear los sistemas que estén comprometidos.