Certified Tech Developer
The Ultimate Degree

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.

Actividad

Deberán leer cada una de las noticias asignadas y responder en un documento de Google Presentations para todas las mesas, las siguientes consignas:

- ¿Qué tipo de amenaza es?

  Backdoor genérico.

- ¿Cómo comienza y cómo se propaga esta amenaza?

  Los operadores tienen varias formas de llegar a una máquina infectada con Kobalos. El método en el cual Kobalos está inmerso en el ejecutable del servidor OpenSSH (sshd) y activará el código del backdoor si la conexión proviene de un puerto de origen TCP específico. Hay otras variantes independientes que no están inmersas en sshd. Estas variantes o se conectan a un servidor C&C que actuará

como intermediario o esperan una conexión entrante en un puerto TCP determinado.

Cualquiera que use el cliente SSH de una máquina comprometida tendrá sus credenciales capturadas. Estas credenciales podrán entonces ser usadas por los atacantes para instalar Kobalos en los nuevos servidores que se descubrieron más tarde.

- ¿Hay más de una amenaza aplicada?

  Solamente tiene la función de ladrón de credenciales SSH. Al menos hasta el momento es la única visible.

- ¿Qué solución o medida recomendarían?

  Configurar el modelo de doble autenticación antes de conectarse a un servidor SSH.

Una vez resueltas, volveremos a la sala principal en la cual el grupo debe compartir sus respuestas a los demás compañeros y compañeras, exponiendo la problemática y el análisis que realizaron.

https://www.welivesecurity.com/la-es/2021/02/02/kobalos-amenaza-linux-afecta-infraestructuras-informaticas-alto-rendimiento/