Mesa 3

Nota : https://www.welivesecurity.com/la-es/2021/04/08/vyveva-nuevo-backdoor-grupo-apt-lazarus/

¿Qué tipo de amenaza es?

Es un tipo de amenaza backdoor del grupo Lazarus

¿Cómo comienza y cómo se propaga esta amenaza?

Hasta el momento no se cuenta con la información completa de como funciona o se propaga, se descubrió un instalador loader y payload principal, un backdoor con una dll de torsocket.. Lo datos de telemetría sugieren que son despliegues de ataques dirigidos, que se encontró en solo dos máquinas y ambas en servidores de una empresa de logística

¿Hay más de una amenaza aplicada ?

El backdoor presenta capacidades para exfiltrar archivos, modificar la fecha de estos (timestomping), recopilar información sobre la computadora de la víctima y sus unidades, y otras funciones comunes de backdoor, cómo ejecutar código arbitrario especificado por los operadores del malware

¿Qué solución o medida recomendarían ?

Aun no se ah efectuado limpieza ,estan en etapa de análisis , por lo que aun no explicaban cómo limpiar