Mesa 3

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

¿Hay más de una amenaza aplicada ?

Principalmente la amenaza está en los comandos que se activan con los cuales se modifican los archivos, y la posibilidad de espionaje en el computador infectado.

¿Qué solución o medida recomendarían ?

A pesar del malware avanzado que usan los piratas informáticos de Lazarus APT, sus ataques aún se pueden mitigar con el uso de un paquete de software anti-malware de buena reputación.

Mesa 3

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

¿Qué tipo de amenaza es?

Malware / Troyano

¿Cómo comienza y cómo se propaga esta amenaza?

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, como ejecutar código arbitrario especificado por los operadores del malware. Esto indica que lo más probable es que el objetivo de esta operación haya sido realizar tareas de espionaje.