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

**¿Qué tipo de amenaza es?**
Spyware, backdoor previamente indocumentado utilizado en un ataque a una empresa de logística de carga en Sudáfrica.

**¿Cómo comienza y cómo se propaga esta amenaza?**
Aunque Vyveva se ha estado utilizando desde al menos diciembre de 2018, aún se desconoce su vector de compromiso inicial. Nuestros datos de telemetría sugieren que ha sido desplegado en ataques dirigidos, ya que solo encontramos dos máquinas víctimas, ambas son servidores propiedad de una empresa de logística de carga ubicada en Sudáfrica

**¿Hay más de una amenaza aplicada ?**
De particular interés son los mecanismos de vigilancia del backdoor, que se pueden habilitar o deshabilitar opcionalmente. Hay un mecanismo de vigilancia de la unidad que se utiliza para monitorear las unidades recientemente conectadas y desconectadas, y otro que monitorea el número de sesiones activas (es decir, usuarios registrados). Estos componentes pueden desencadenar una conexión con el servidor C&C fuera del intervalo regular preconfigurado de tres minutos y en eventos de sesiones y/o unidades nuevas.

**¿Qué solución o medida recomendarían ?**
No instalarlo