GRUPO 3
https://www.welivesecurity.com/la-es/2021/04/08/vyveva-nuevo-backdoor-grupo-apt-lazarus/

¿Qué tipo de amenaza es?
Es un malware. Es un troyano.
¿Cómo comienza y cómo se propaga esta amenaza?
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. 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.

¿Hay más de una amenaza aplicada?
Una vez activo, el troyano Vyveva Backdoor se conecta a un servidor de control remoto y escucha activamente nuevas instrucciones. Los operadores maliciosos pueden ejecutar una gran cantidad de comandos predefinidos, que les permiten:

Modificar y guardar archivos.
Obtenga información sobre la configuración y el contenido de la partición de la unidad.
Sube archivos o carpetas al servidor de control.
Lista de archivos de carpeta.
Gestionar procesos en ejecución.
Auto destrucción.

¿Qué solución o medida recomendarían?
Lo mejor para protegernos de un backdoor es contar con un buen antivirus que ofrezca protección en tiempo real, que además se mantenga actualizado con regularidad para poder detectar nuevas amenazas y, por supuesto, tener activada la protección de manera permanente. En el mercado existen varias opciones, tanto de pago como gratuitas, aunque serán las de pago las más completas de cara a la protección de nuestros equipos.

Además de contar con esta protección, por supuesto también está el uso del sentido común y la precaución a la hora de navegar por Internet y descargarnos archivos; si una página no es de confianza o te resulta sospechosa, no entre en ella, si tu antivirus te avisa de algún peligro, no entres en ella y, sobre todo, no descargues archivos de lugares poco confiables o de remitentes desconocidos, o archivos sospechosos de conocidos.