● ¿Qué tipo de amenaza es?

El tipo de amenaza de Vyveva de malware es del tipo troyano Backdoor

● ¿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. Se prevé 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. Este hecho pareciera que puede ser un ataque dirigido con ingeniería social

● ¿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.