**Mesa 3**

**Juan Ignacio Castore Thiago Viera Lia Belen Dominguez**

Nota:

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

¿Qué tipo de amenaza es?

*Es un Backdoor que llamaron Vyveva. Un backdoor es un tipo de troyano que permite el acceso al sistema infectado y su control remoto. El atacante puede entonces eliminar o modificar archivos, ejecutar programas, enviar correos masivamente o instalar herramientas maliciosas.*

¿Cómo comienza y cómo se propaga esta amenaza?

Ingresa a través de una secuencia especial o un término trasero dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad del algoritmo (autentificación) para acceder al sistema.

Se introducen en el sistema gracias a otros programas nocivos como [troyanos](https://www.pandasecurity.com/es/security-info/trojan/), [virus](https://www.pandasecurity.com/es/security-info/virus/) o incluso spyware. Consiguen acceso sin que el administrador se de cuenta y luego infectan las sesiones a cada uno de los usuarios conectados a la red comprometida. Es posible que algunas amenazas puedan ser colocadas con carácter previo por usuarios que tienen los privilegios adecuados, para ganar acceso más tarde.

¿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, 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.

¿Qué solución o medida recomendarían?

Primero, hay que tener cuidado con lo que descargamos y tambien tener un buen antivirus. Para eliminarlo recurrimos al antivirus o algun programa de limpieza