**Clase 24 amenazas**

**Mesa 3:** Link: <https://www.welivesecurity.com/la-es/2021/04/08/vyveva-nuevo-backdoor-grupo-apt-lazarus/>

* **¿Qué tipo de amenaza es?**

Este backdoor consta de varios componentes y se comunica con su servidor de C&C a través de la red Tor

* **¿Cómo comienza y cómo se propaga esta amenaza?**

Vyveva usa la biblioteca Tor, que se basa en el código fuente oficial de Tor, para comunicarse con un servidor de C&C seleccionado al azar de la configuración. Se pone en contacto con el C&C en intervalos de tres minutos, enviando información sobre la computadora de la víctima y sus unidades antes de recibir comandos. El directorio de exportación del backdoor contiene el TorSocket.dll con exportaciones que se explican solas close\_ch, connect\_ch, open\_ch, read\_ch, write\_ch.. 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?**

Se encontraron en dos máquinas víctimas, ambas son servidores propiedad de una empresa de logística de carga ubicada en Sudáfrica.

* **¿Qué solución o medida recomendarían?**

Sus ataques se pueden mitigar con el uso de un paquete de software anti-malware de buena reputación