# BOLETÍN DE ALERTA

**Boletín Nro.**: 2021-23

**Fecha de publicación**: 17/09/2021

**Tema**: Descifrador del ransomware REvil/Sodinokibi.

**Productos afectados:**

- Archivos encriptados  por el ransomware REvil/Sodinokibi.

**Descripción:**

Se ha publicado un descifrador del ransomware REvil/Sodinokibi, que permite a las víctimas de ataques realizados antes del 13 de julio de 2021 restaurar sus archivos sin pagar a los ciberdelincuentes. Ha sido desarrollado por Bitdefender junto con un socio policial no revelado, la herramienta de descifrado se puede descargar del sitio web de Bitdefender de forma gratuita.

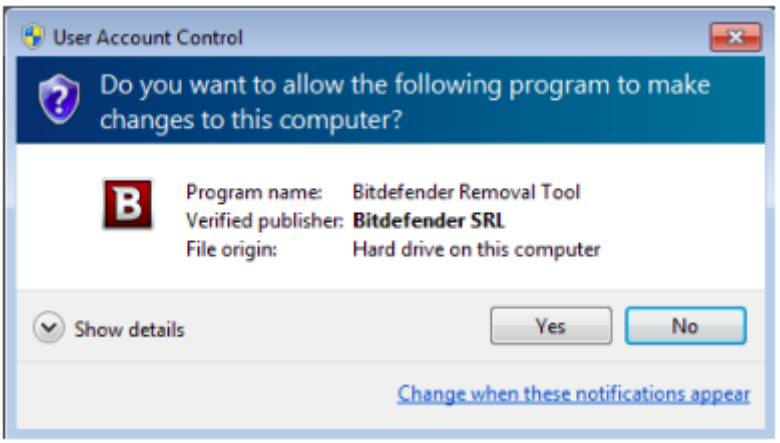
**REvil** es un operador de **Ransomware-as-a-Service (RaaS)** probablemente con sede en un país de la Comunidad de Estados Independientes (CEI). Surgió en 2019 como sucesor del ahora desaparecido ransomware GandCrab y es uno de los ransomware más prolíficos en la Dark Web, ya que sus afiliados se han dirigido a miles de empresas de tecnología, proveedores de servicios gestionados y minoristas de todo el mundo.

Si usted o su organización ha sido afectada por el ransomware REvil, debe seguir los siguientes pasos para descifrar los archivos comprometidos.

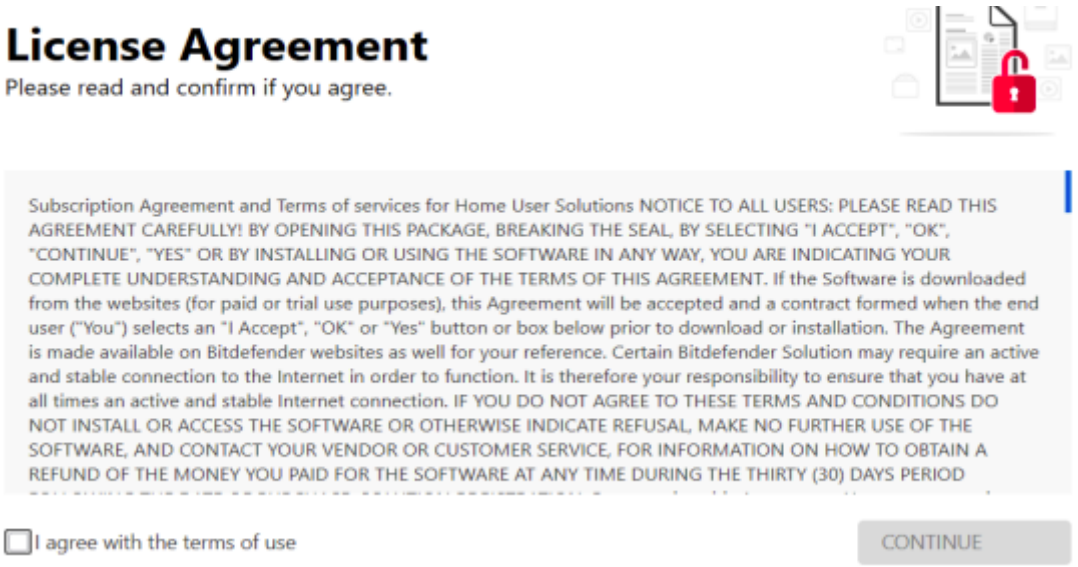
**Pasos para el descifrado:**

**Paso 1:** descargue la herramienta de descifrado desde:
http://download.bitdefender.com/am/malware_removal/BDREvilDecryptor.exe

**Paso 2:** haga doble clic en el archivo y permita que se ejecute haciendo clic en **"Yes"** en el mensaje de UAC.



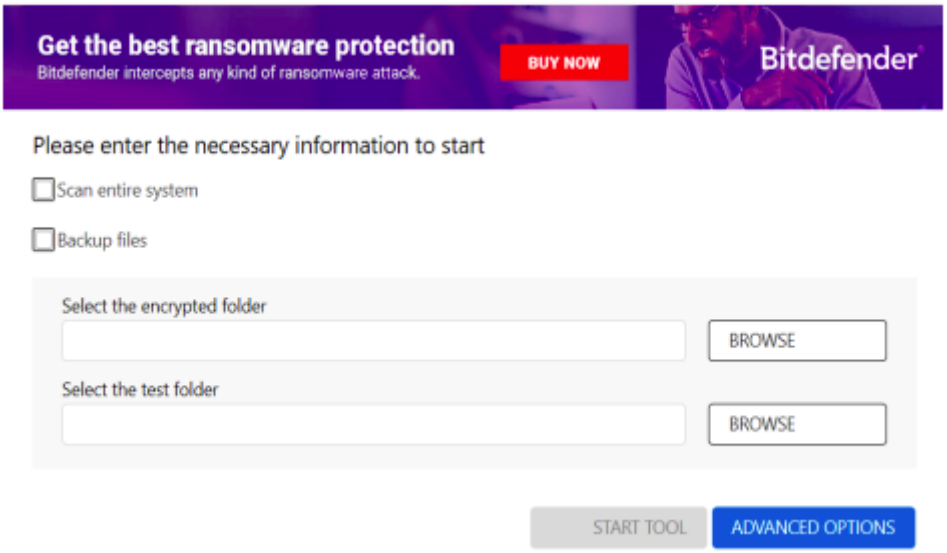

**Paso 3:** seleccione "I Agree" para aceptar el Acuerdo de Licencia de Usuario Final.



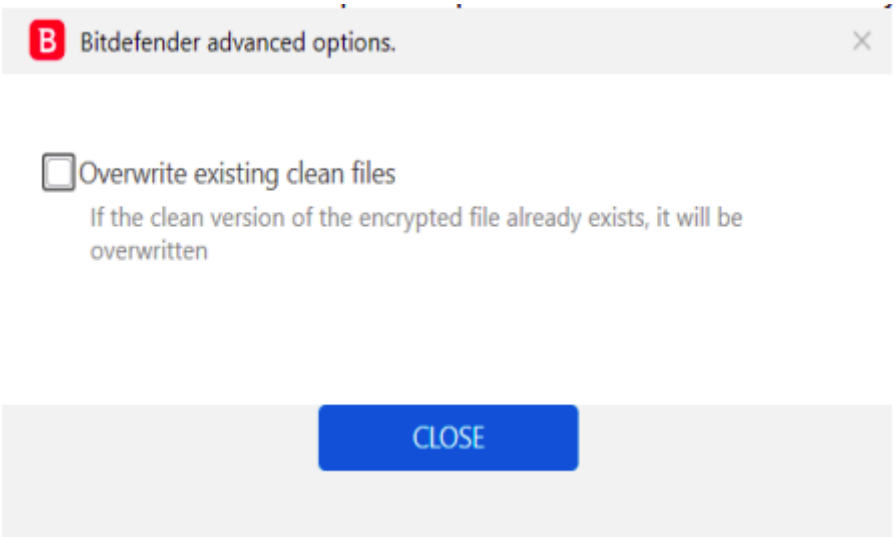

**NOTA:** Algunas versiones aún no se pueden descifrar.

**Paso 4:** Seleccione **"Scan Entire System"** si desea buscar todos los archivos cifrados o simplemente agregar la ruta a sus archivos cifrados.

Recomendamos encarecidamente que también seleccione **"Backup files"** antes de iniciar el proceso de descifrado. Luego presione **"Scan"**.




Los usuarios también pueden marcar la opción de **“Overwrite existing clean files”** en **“Advanced options”** para que la herramienta sobreescriba los posibles archivos limpios actuales con su descifrado equivalente.




Al finalizar este paso, sus archivos deberían haber sido descifrados.

**Recomendaciones finales:**

- Si tiene algún problema, contacte a forensics@bitdefender.com.
- Si marcó la opción de copia de seguridad, verá los archivos cifrados y descifrados.
- También puede encontrar un registro que describe el proceso de descifrado, en la carpeta **%temp%\BDRemovalTool**.
- Para deshacerse de los archivos encriptados, simplemente busque los archivos que coincidan con la extensión y elimínalos de forma masiva. No le recomendamos que haga esto, a menos que haya comprobado dos veces que sus archivos se pueden abrir de forma segura y que no haya rastros de daños.

**Información adicional:**

- https://www.bitdefender.com/blog/labs/bitdefender-offers-free-universal-decryptor-for-revil-sodinokibi-ransomware/
- https://www.bleepingcomputer.com/news/security/free-revil-ransomware-master-decrypter-released-for-past-victims/