How to recover files encrypted by REvil / Sodinokibi Ransomware

This article will guide you stepwise through how to use Bitdefender's free decryption tool to recover files encrypted by the REvil / Sodinokibi ransomware.

What is REvil ransomware?

REvil is a Ransomware-as-a-Service (RaaS) operator likely based in a Commonwealth of Independent States (CIS) country. It emerged in 2019 and is one of the most prolific ransomwares on the Dark Web as affiliates have targeted thousands of technology companies, managed service providers, and retailers around the world. After successfully encrypting a business' data, REvil affiliates demand large ransoms up to US $70 million in exchange for a decryption key and the assurance they will not publish the internal data exfiltrated during the attack.

For the best protection, we recommend that you always keep Bitdefender's Ransomware Remediation module and the Automatic restore feature active. When the Automatic restore option is enabled, Bitdefender automatically restores files that were encrypted by ransomware. Hereby, you can enjoy a worry-free experience knowing that your files are safe. To learn more about Bitdefender's Ransomware Remediation and how it can help you recover ransomware encrypted files check out this article – What is Bitdefender Ransomware Remediation and how does it work?

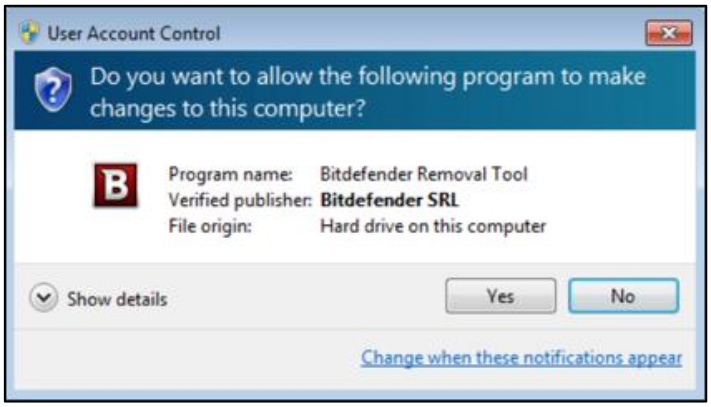
How to recover files encrypted by REvil ransomware

Step 1: Download the REvil ransomware decryption utility from here:

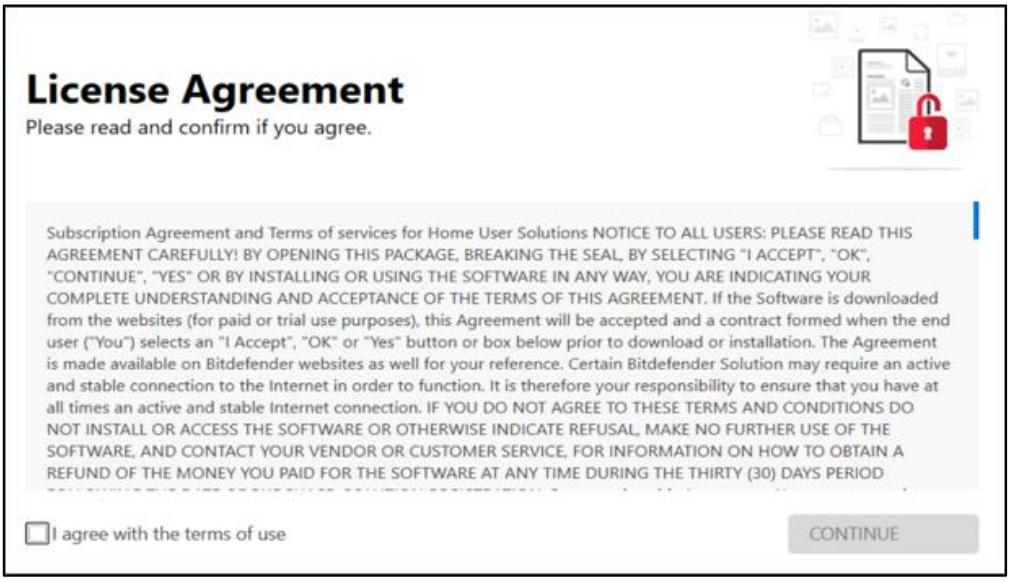
https://download.bitdefender.com/am/malware_removal/BDREvilDecryptor.exe

and save it on the ransomware-affected computer.

Step 2: Double-click the downloaded file BDREvilDecryptor.exe and allow it to run by clicking Yes in the User Account Control dialog box.



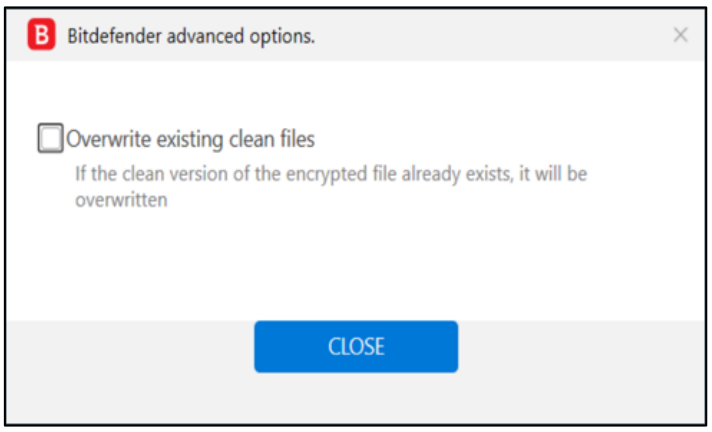
Step 3: Select “I Agree” after you read and agree with the License Agreement. Then press CONTINUE.



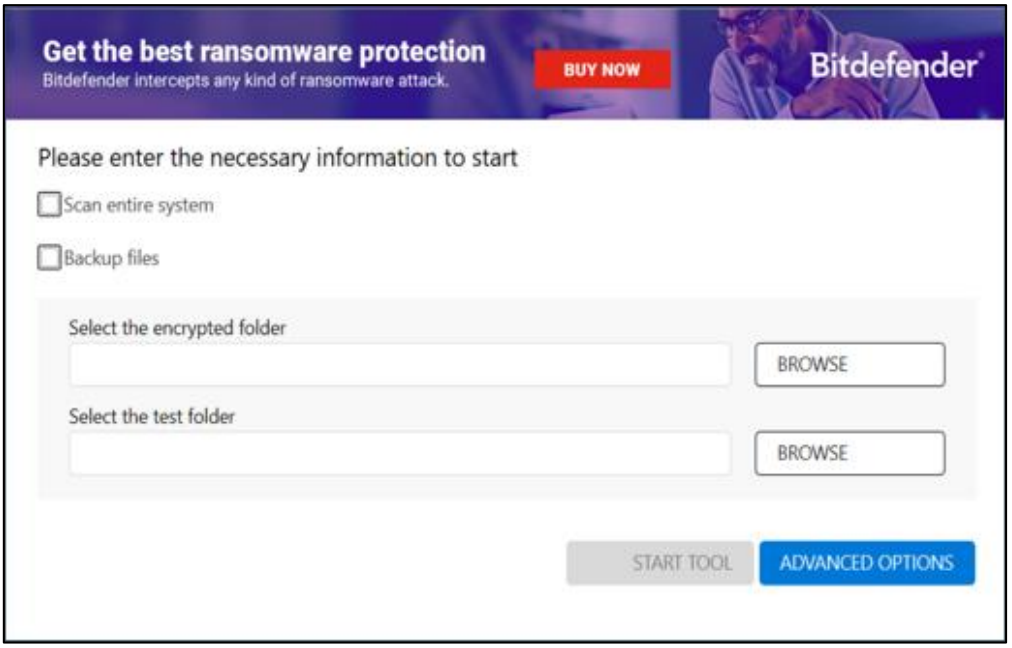
Step 4: Check the “Scan Entire System” box if you want the Bitdefender utility to scan your entire computer for REvil ransomware encrypted files. Alternatively, you can use the BROWSE button to manually select the folder where you know the encrypted data is located.

We strongly recommend that you also check the “Backup files” box before starting the decryption process.

You can also check the “Overwrite existing clean files” option under ADVANCED OPTIONS, so the tool will overwrite any existing clean files with their decrypted equivalent.



Then press the START TOOL button.



After a short wait, your files should be decrypted.

Note: If you tick the backup option, you will see both encrypted and decrypted files.

You can also find a log describing the decryption process inside the *%temp%\BDRDRemovalTool* folder. To get rid of the remaining encrypted files, just search for files matching the extension and remove them in bulk. We don’t encourage you to do this until you double-check your decrypted files can be opened and that there is no sign of damage.