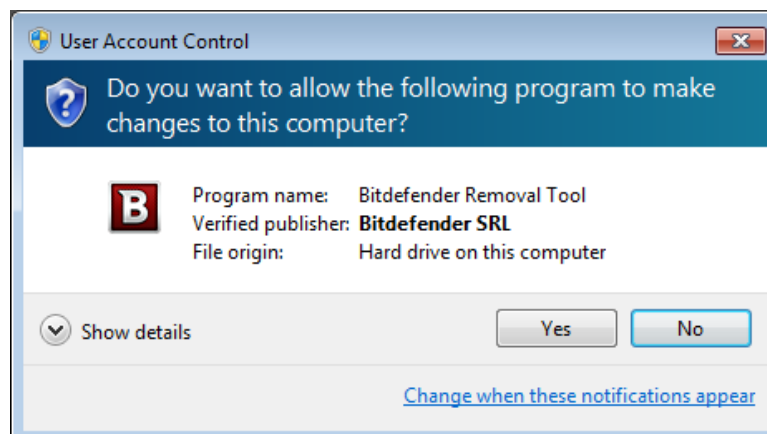# REvil RANSOMWARE DECRYPTION TOOL

Steps for decryption:

Step 1: Download the decryption tool from
download.bitdefender.com/am/malware_removal/BDREvilDecryptor.exe
and save it somewhere on your computer

Step 2: Double-click the file and allow it to run by clicking Yes in the UAC prompt.

Step 3: Select "I Agree" for the End User License Agreement

NOTE: Some versions are not yet decryptable
Step 4: Select "Scan Entire System" if you want to search for all encrypted files or just add the path to your encrypted files.

We strongly recommend that you also select "Backup files" before starting the decryption process. Then press "Scan".

Please enter the necessary information to start

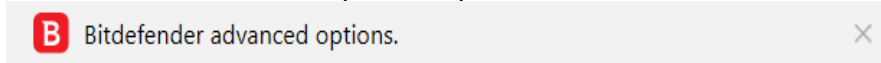☐ Scan entire system

☐ Backup files

Select the encrypted folder

[   ]   [BROWSE]

Select the test folder

[   ]   [BROWSE]

[START TOOL]   [ADVANCED OPTIONS]

Users may also check the "Overwrite existing clean files" option under "Advanced options" so the tool will overwrite possible present clean files with their decrypted equivalent.

B Bitdefender advanced options.   ✕

☐ Overwrite existing clean files
If the clean version of the encrypted file already exists, it will be overwritten

[CLOSE]
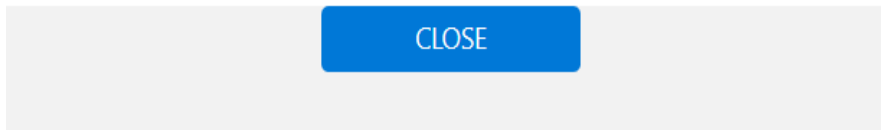
At the end of this step, your files should have been decrypted.

If you encounter any issues, please contact us at forensics@bitdefender.com.
If you checked the backup option, you will see both the encrypted and decrypted files. You can also find a log describing decryption process, in **%temp%\BDRemovalTool** folder:

To get rid of your left encrypted files, just search for files matching the extension and remove them bulk. We do not encurage you to do this, unless you doubled check your files can be opened safely and there is no trace of damage.

Silent execution (via cmdline)
The tool also provides the possibility of running silently, via a command line. If you need to automate the deployment of the tool inside a large network, you might want to use this feature.

- **-help** - will provide information on how to run the tool silently (this information will be written in the log file, not on console)
- **start** - this argument allows the tool to run silently (no GUI)
- -**path** - this argument specifies the path to scan
- **o0:1** - will enable **Scan entire system** option (ignoring **-path** argument)
- **o1:1** - will enable **Backup files** option
- **o2:1** - will enable **Overwrite existing files** option

Examples:

BDREvilDecryptor.exe start -path:C: -> the tool will start with no GUI and scan **C:**
BDREvilDecryptor.exe start o0:1 -> the tool will start with no GUI and scan entire system
BDREvilDecryptor.exe start o0:1 o1:1 o2:1 -> the tool will scan the entire system, backup the encrypted files and overwrite present clean files

Acknowledgement:
This product includes software developed by the OpenSSL Project, for use in the OpenSSL Toolkit (http://www.openssl.org/)