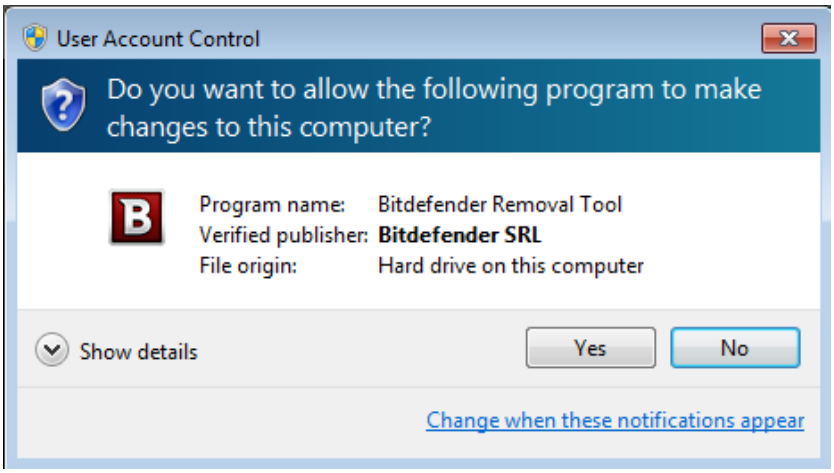
MegaCortex RANSOMWARE DECRYPTION TOOL

Important note: In case of encryption with versions 2-4, please make sure the system contains the ransom note (e.g. “!!_READ_ME_!!!.TXT”, “!-!_README_!-!.RTF”, etc). For encryption with MegaCortex V1 (the encrypted files have the “.aes128ctr” extension appended), please ensure the ransom note and TSV log file (e.g. “fracxidg.tsv”) created by the ransomware are present on the system.

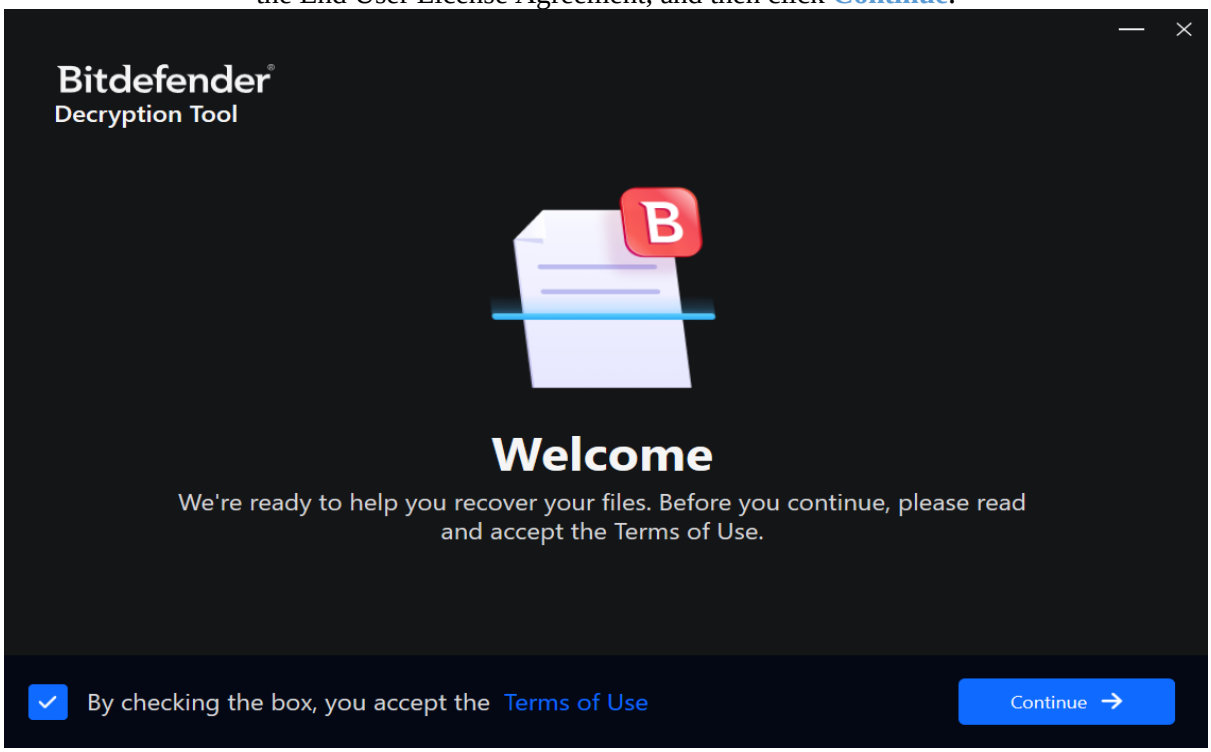
Steps for decryption:

Step 1: Download the decryption tool from https://download.bitdefender.com/am/malware_removal/BDMegaCortexDecryptTool.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: Read the Terms of Use and select **“By checking the box, you accept the Terms of Use”** for the End User License Agreement, and then click **Continue**.



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 maintain the “Backup files” option enabled. Then press “**Start now**”.

Users may also check the “Replace previously decrypted files” option under “Advanced options”, so the tool will replace already decrypted files.

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

If you encounter any issues, please contact us at forensics@bitdefender.com or https://www.bitdefender.com/consumer/support/help/ .

If you check the backup option, you will see both the encrypted and decrypted files. You can also find a log describing decryption process, in **%temp%\BitdefenderLog.txt** folder:

To get rid of your left encrypted files, just search for files matching the extension and remove them. Before doing so, please make sure you have checked that the files have been properly decrypted.

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)
- **-scan-path** - this argument specifies the path containing encrypted files
- **-full-scan** - will enable the **Scan entire system** option (ignoring **-scan-path** argument)
- **-disable-backup** - will disable the file Backup option
- **-replace-existing** - will enable the Replace previously decrypted files option

Examples:

BDMegaCortexDecryptTool.exe start -scan-path:C: -> the tool will start with no GUI and scan **C:**
BDMegaCortexDecryptTool.exe start -full-scan -> the tool will start with no GUI and scan entire system
BDMegaCortexDecryptTool.exe start -full-scan -replace-existing -> the tool will scan the entire system 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/)