

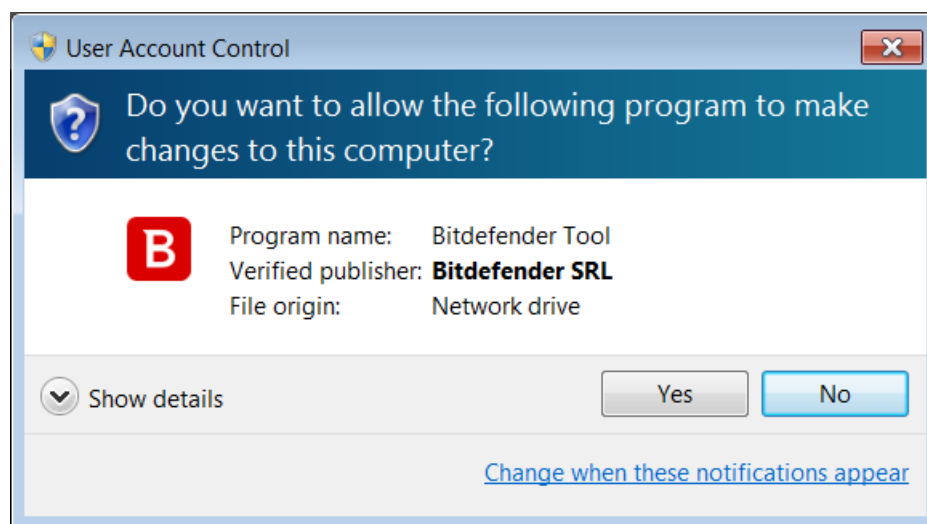
DarkSide Ransomware Decryption Tool

Step 1: Download the decryption tool and save it somewhere in your computer from:

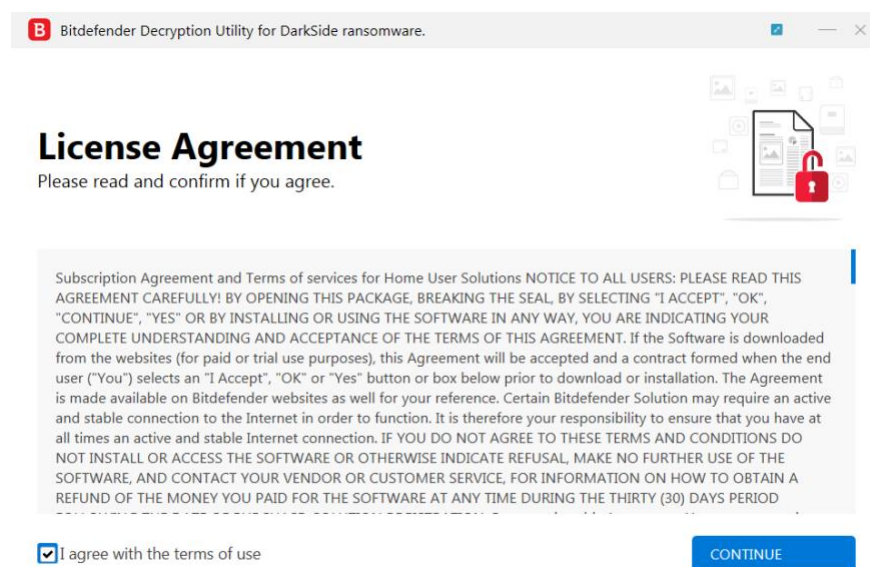
http://download.bitdefender.com/am/malware_removal/BDDarkSideDecryptor.exe

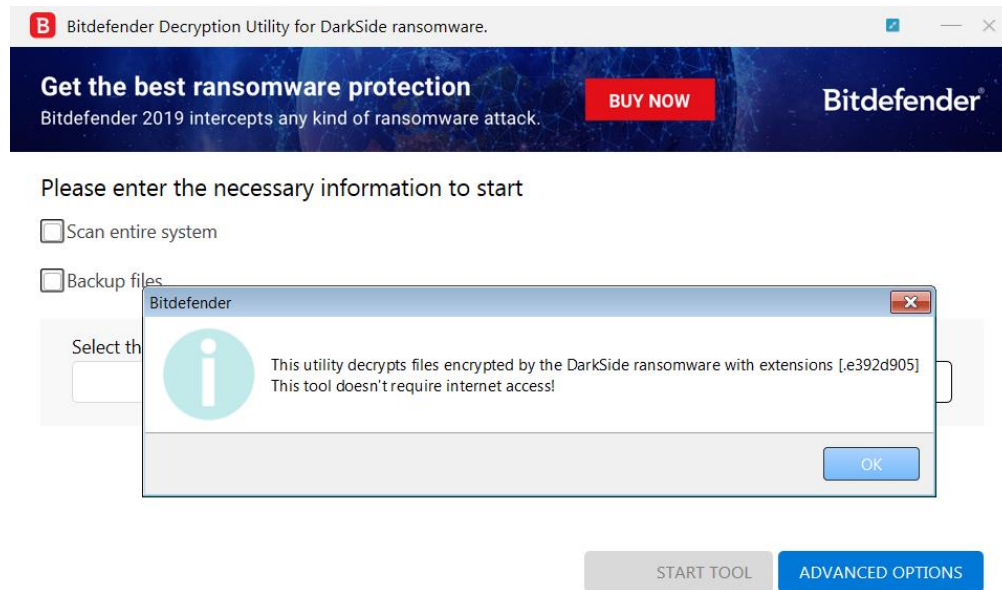
This tool works on an infected pc that has an active internet connection.

Step 2: Double click BDDarkSideDecryptor.exe and allow it to run by clicking yes on the UAC alert.



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

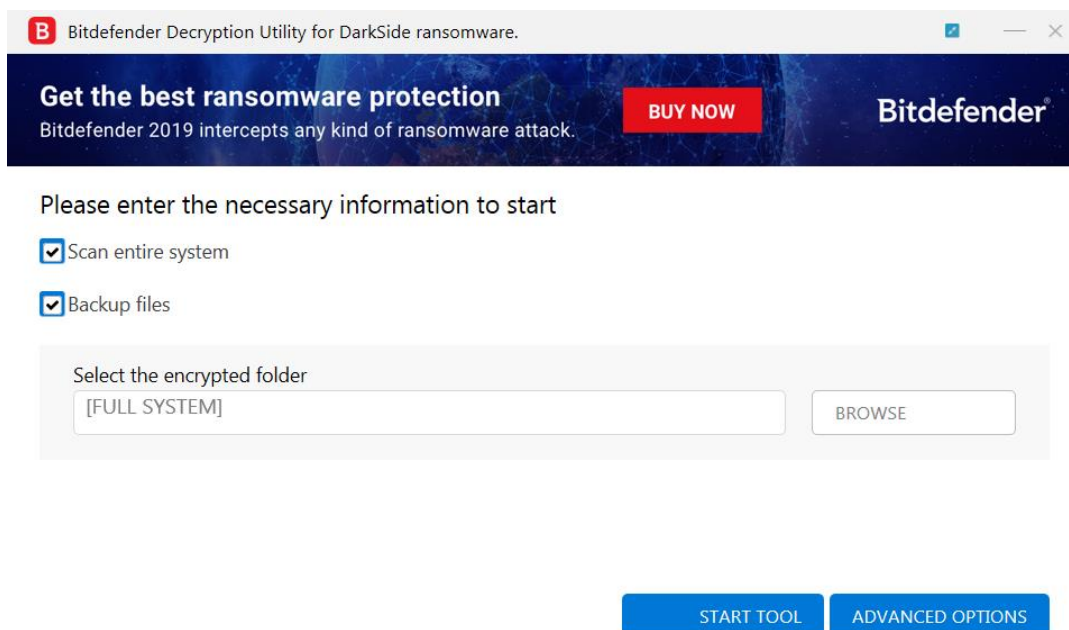




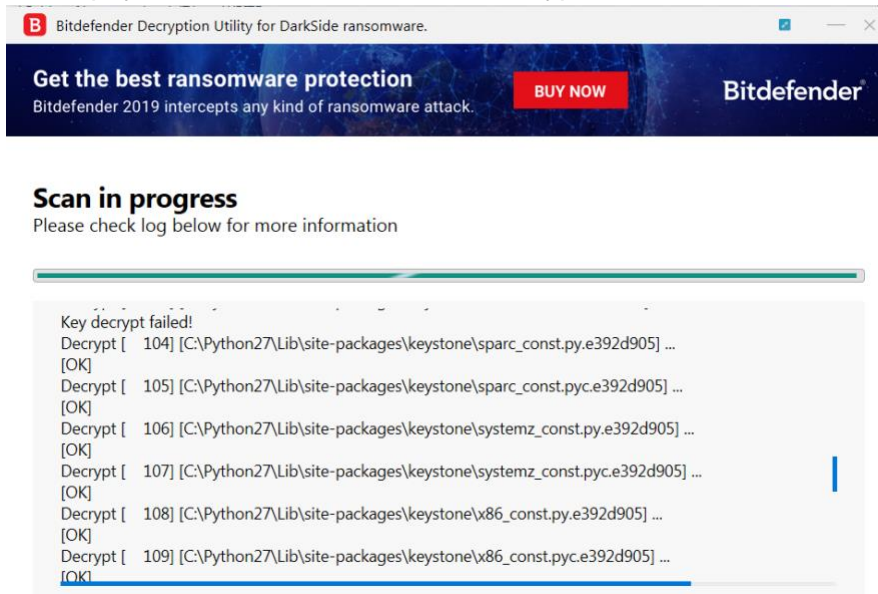
Note: Tool informs that encrypted files extension, for the current PC, should be *.e392d905, please check that you have encrypted files, with this extension, otherwise no files will be decrypted.

Step 4: Select “Scan Entire System” if you want to search for all encrypted files or just add the path to where you previously saved the encrypted files.

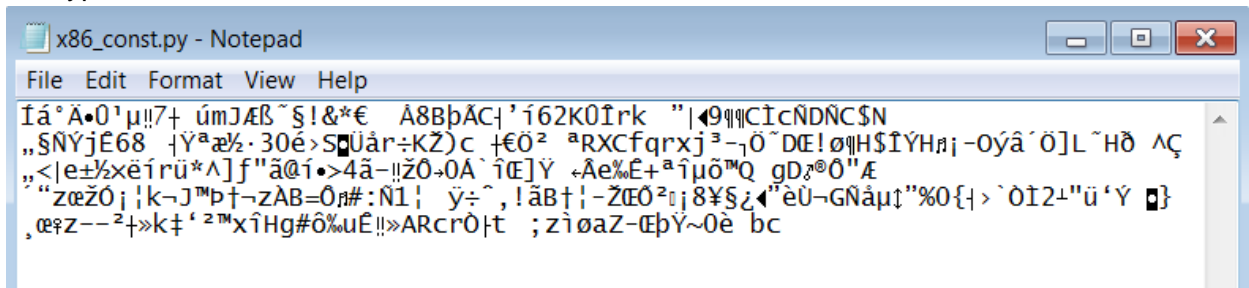
We strongly recommend that you also select “Backup files” before starting the decryption process in case anything unwanted happens while decrypting. Then press “Start Tool”.



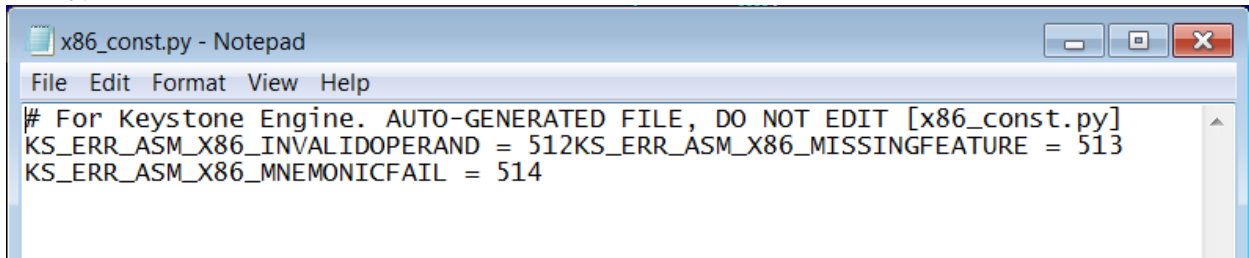
At the end of this step, your files should have been decrypted.



Encrypted:



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 encourage you to do this, unless you doubled check your files can be opened safely and there is no trace of damage.

Ransomware in some cases encrypts files incorrectly so that decryption will not work properly, we recommend that you back up your files before using the decryption tool if you have not already checked the option "backup files " from decryption tool.

Acknowledgement:

This product may include software developed by the OpenSSL Project, for use in the OpenSSL Toolkit (<http://www.openssl.org/>)