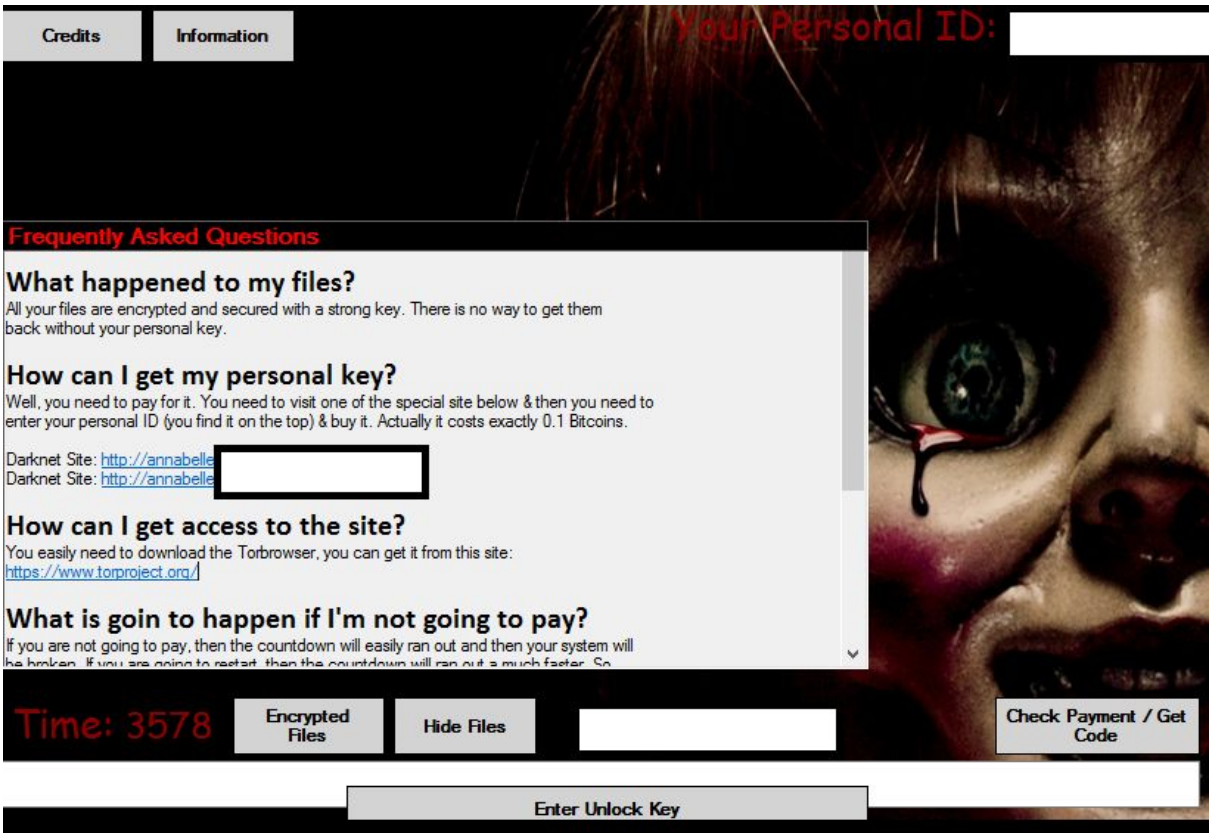
Annabelle RANSOMWARE DECRYPTION TOOL

Introduction: This tool decrypts files encrypted by Annabelle ransomware. You can recognize this ransomware by the extension it appends to the encrypted files: (.ANNABELLE).:

clean.hivu.ANNABELLE

The tool is available for download at the following address:
http://download.bitdefender.com/am/malware_removal/BDAnnabelleDecryptTool.exe

Ransom-note:



Annabelle encrypts user files using AES256 CBC with a hardcoded key and IV.

Example of encrypted files:

autoruns.arn.ANNABELLE	2/23/2018 2:36 PM	ANNABELLE File	7,120 KB
clean.hivu.ANNABELLE	2/23/2018 2:36 PM	ANNABELLE File	122,798 KB

NOTE 1: the malware locks the screen of the pc in the first phase and changes the MBR in the second phase. In order to be able to use the tool, the user should do the following :

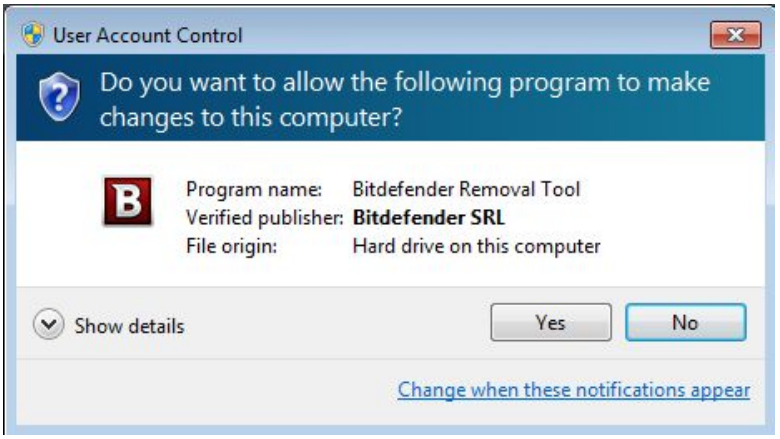
- **recover the MBR(replacement / change if possible via various tools)**
- **delete the registry keys and the malware remainans offline / rescue-CD**
- **use BDAnnabelleDecryptor tool to decrypt the files**

NOTE 2: due to the encryption using AES, the size of the result message will be a multiple of 16 bytes. Therefore, upon decryption, there is a chance that a few bytes will remain at the end of the file (max 15). This should not affect the file and they cannot be removed during decryption since there is no mark of the original file size.

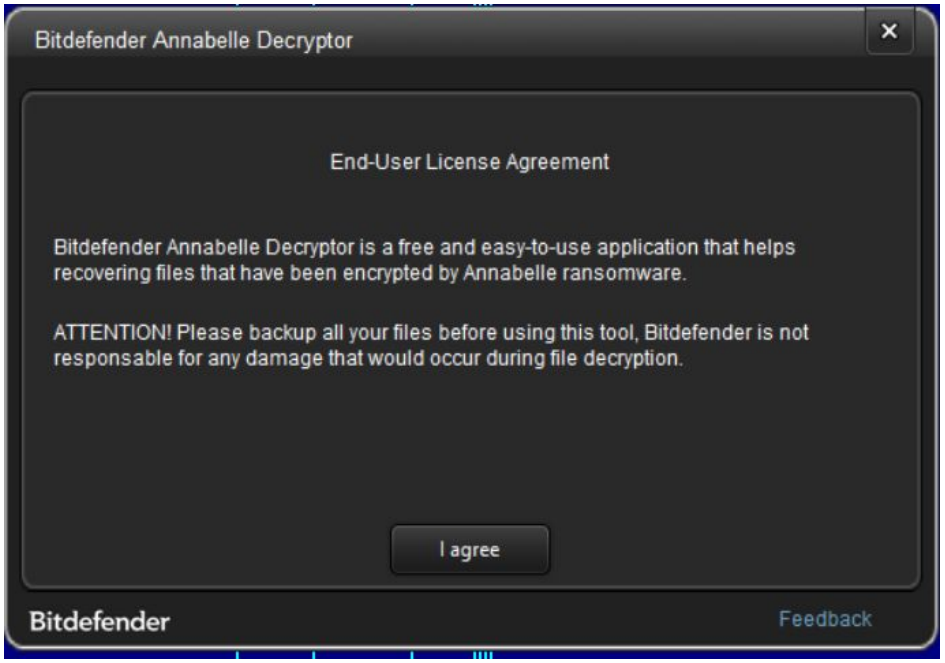
Steps for decryption:

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

Step 2: Double-click the file (previously saved as BDAnnabelleDecryptor.exe) and allow it to run by clicking Yes in the UAC prompt.

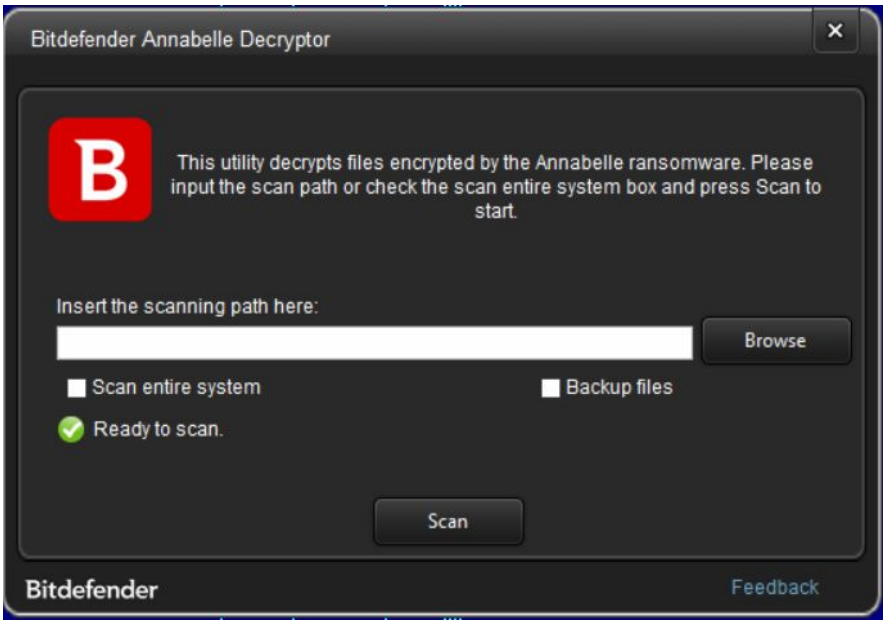


Step 3: Select “I Agree” for the End User License Agreement



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, should anything occur while decrypting. Then press “Scan”.



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:

Acknowledgement:

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