# Decrypted: Rhysida Ransomware

# Usage of the Decryptor

**Please, read the following instructions carefully. The rate of success depends on them.**

**Several parameters of the infected PC affect the encryption (and decryption) of the files:**

- Set of the drive letters
- Order of files
- Number of CPU cores
- Bitness of the executed ransomware sample
- Format of files before encryption

**For these reasons, the following rules must be obeyed while decrypting files:**

- The decryptor must be executed on the same machine where the files were encrypted
- Password cracking process must be executed on the same machine where the files were encrypted
- No files from another machine can be copied to the machine where the decryption process is performed
- Text files (source files, INI files, XML, HTML, …) must have certain minimal size to be decryptable

64-bit samples of the Rhysida encryptors are far more common. For that reason, default configuration of the decryptor assumes 64-bit encryptor. If you are sure that it was 32-bit version (for example, if you have 32-bit operating system), the decryptor can be switched to 32-bit mode by using the following command line parameter:

**avast_decryptor_rhysida.exe /ptr:32**

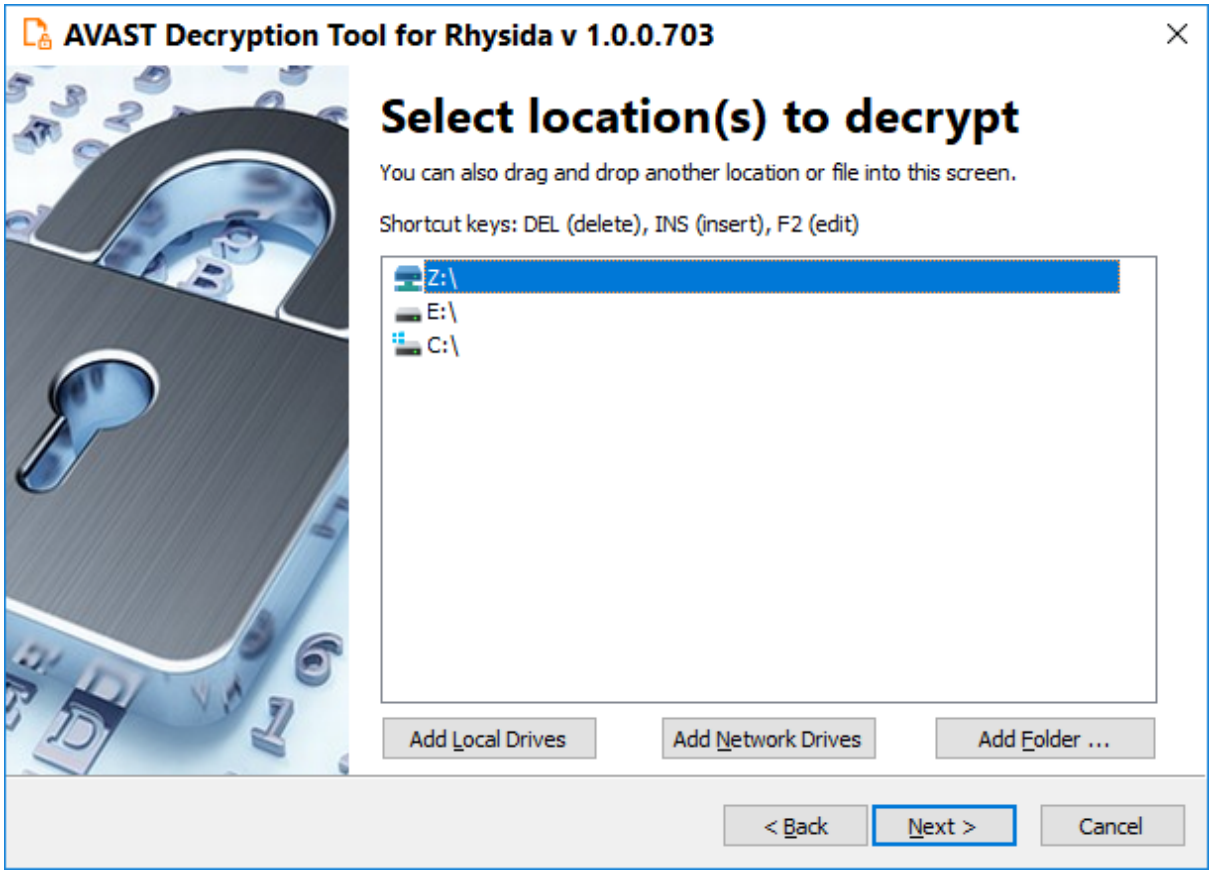
If you want to verify whether the decryption process will work without changing the files, you may use the “testing mode” of the decryptor. This mode is activated by the following command line parameter:

**avast_decryptor_rhysida.exe /nodecrypt**

The Rhysida decryptor also relies on the known file format. Common file formats, such as Office documents, archives, pictures, and multimedia files are already covered. If your encrypted data includes valuable documents in less common or proprietary formats, please, contact us at decryptors@avast.com. We can analyze the file format and if possible, we add its support to the decryptor.

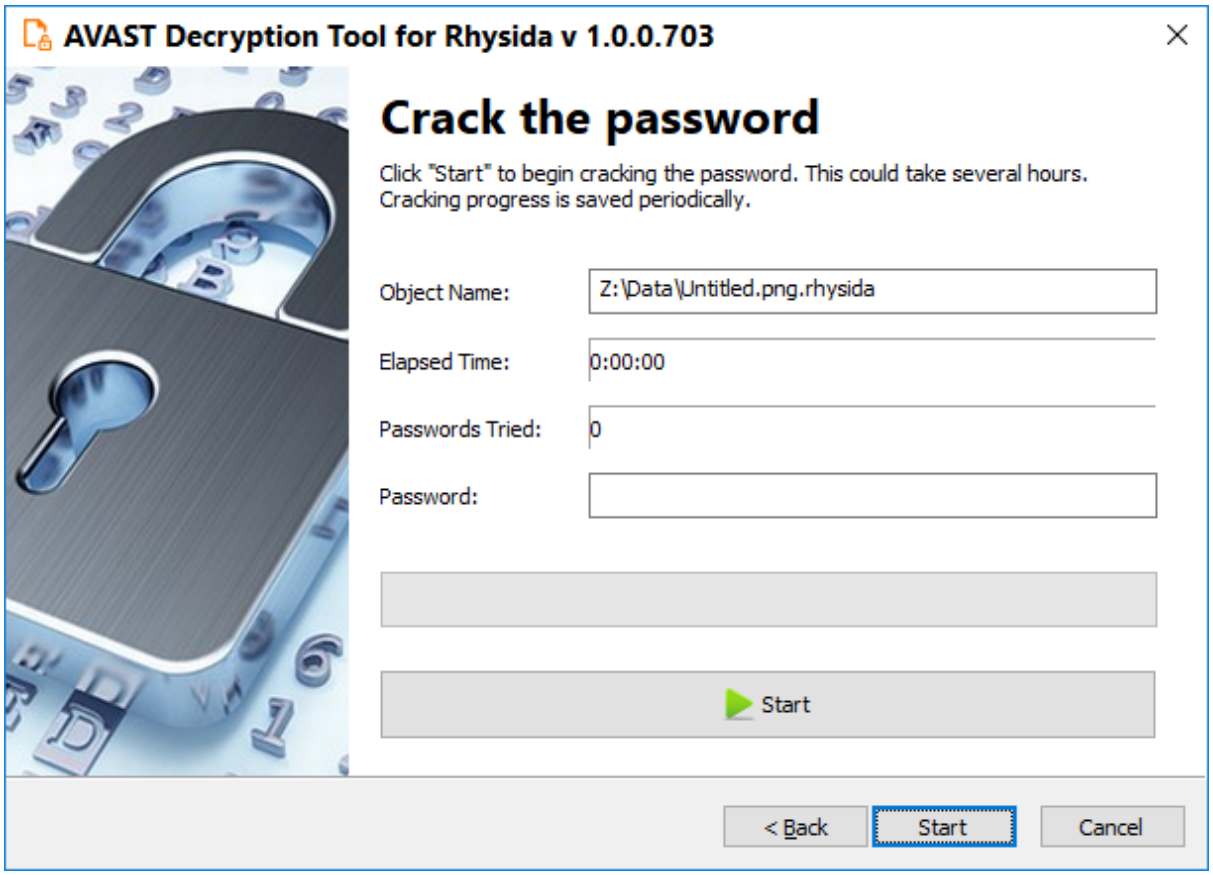
1. Download the decryptor here.
2. Run the decryptor. Unless you need one or more command line modifications, you can simply run it by clicking on the downloaded file.
3. On the initial page, you must confirm that you are running the decryptor on the same PC where the files were encrypted. Click Yes, then the Next button when you are ready to start.


4. Next page shows the list of drive letters on the PC. You may notice that it is in reverse order. Please, keep it as it is and click “Next.”




5. The next screen requires you to enter an example of an encrypted file. In most cases, the decryptor picks the best file available for the password cracking process.

6. The next page is where the password cracking process takes place. Click Start when you are ready to begin. This process usually only takes a few seconds but will require a large amount of system memory.




7. Once the password is found, you can continue to decrypt all the encrypted files on your PC by clicking Next:

8. On the final page, you can opt-in to back up your encrypted files. These backups may help if anything goes wrong during the decryption process. This choice is selected by default, which we recommend. After clicking Decrypt the decryption process begins. Let the decryptor work and wait until it finishes decrypting all of your files.


For questions or comments about the Avast decryptor, email decryptors@avast.com.