Free Decryptor for the Chaos ransomware

User Manual

Truesec AB
Oxtorgsgränd 2, 111 57 Stockholm

hello@truesec.com
www.truesec.com

TRUESEC

Table of Contents

Truesec Group
Corp. ID: 556690-8074
www.truesec.com

Sweden
+ 46 810 00 10
hello@truesec.com

Denmark
+ 46 810 00 10
hello@truesec.com

US
+1 (904) 900-4532
hello@truesec.com

1. Change History

Version	Date	Description
0.1	2022-09-16	First Draft
0.2	2022-09-19	Quality Review
1.0	2022-09-19	First Release

Table 1 Change History

2. Background

2.1 The decryption software

This is a free software that helps you recover files encrypted by the Chaos ransomware family.

BEFORE USING THIS SOFTWARE, YOU MUST CAREFULLY READ THIS USER MANUAL.

This software is listed on the "No More Ransom" project, an initiative by Europol's ECC, et. al., with the goal to help victims of ransomware retrieve their encrypted data without having to pay the criminals.

This software is provided by Truesec and is distributed under GPLv3. Truesec is a global cyber security company that covers the entire cybersecurity spectrum. Our incident response team performs hundreds of complex cyber incident investigations every year. Founded in Sweden, we have been delivering cutting-edge solutions to both the private and public sectors since 2005.

2.2 Chaos ransomware family

The *Chaos ransomware family* is a set of malicious software, which are derived from the same original malicious software. The Chaos ransomware was first published at 2021-06-09, under the name *Ryuk .Net Ransomware Builder*. The author later rebranded the builder to *Chaos Ransomware Builder*. The builder has been constantly updated since then, and multiple forks have been observed such as *Minecraft alt*[1] and *WannaFriendMe*. [2]

The ransomware group *Onyx* first appeared in in April 2022. The ransomware group use a fork of the Chaos ransomware. The group changed its name to *VSOP* in August 2022.

Around May 2022, a ransomware known as *Yashma/AstraLocker* appeared, that was based on Chaos ransomware. The group officially shutdown in July 2022 and published a free decryptor. [3]

In August 2022, a ransomware-as-a-service named *Solidbit* appeared that is also based on a Chaos fork.[4]

[1] https://www.fortinet.com/blog/threat-research/chaos-ransomware-variant-in-fake-minecraft-alt-list-brings-destruction
[2] https://www.bleepingcomputer.com/news/security/roblox-game-pass-store-used-to-sell-ransomware-decryptor/
[3] https://www.bleepingcomputer.com/news/security/free-decryptor-released-for-astralocker-yashma-ransomware-victims/
[4] https://www.varonis.com/blog/anatomy-of-a-solidbit-ransomware-attack

Truesec Group
Corp. ID: 556690-8074
www.truesec.com

Sweden
+ 46 810 00 10
hello@truesec.com

Denmark
+ 46 810 00 10
hello@truesec.com

US
+1 (904) 900-4532
hello@truesec.com

2.3 Chaos ransomware

The early versions of Chaos are essentially wiper ware. All files smaller than 2,117,152 bytes (2MB) and in some cases even 1 MB are destroyed. There is no possibility to decrypt these files because they are *removed* and not encrypted.

In more recent versions, the limit is configurable and can vary. You should review the specific sample that affected your organization.

Truesec Group
Corp. ID: 556690-8074
www.truesec.com

Sweden
+ 46 810 00 10
hello@truesec.com

Denmark
+ 46 810 00 10
hello@truesec.com

US
+1 (904) 900-4532
hello@truesec.com

3. Preparations

This section contains the preparation steps needed to run this decryption software. Please read the instructions carefully to avoid data loss and unexpected results. These steps are **mandatory.**

3.1 Perform a full disk backup

Take a full backup of the entire drive ***before*** running the decryptor.

The ransomware *removes* large files, and these could potentially be carved by a file recovery utility. Therefore, it is very important to preserve the free space on the drive.

3.2 Remove the ransomware persistence

The ransomware creates various types of persistence, depending on the strain and configuration. Persistence techniques include startup folder items, scheduled tasks, system services, and autorun registry keys. You must **manually** remove any persistence on your system. Failure to do so will result in your system being encrypted once again.

In general, a decryptor software does not replace the need of a proper forensic investigation. We urge you to perform containment, forensic investigation, and remediation activities to secure your environment from further damage.

3.3 Stop the ransomware process

Before running the decryptor, you must ensure that the ransomware process is no longer running.

3.4 Disk space and permissions

The decryptor software needs to have read/write permission to the files/folders you want to decrypt. The decryptor will create a new decrypted file for each encrypted file, therefore we recommend that you have at least 50% free disk space on the target volume.

3.5 Obtain the decryptor software

Please follow the link listed on https://nomoreransom.org to download the decryptor software.

Optionally, you can build the decryptor from source. See the readme in the Github repository for further instructions.

Truesec Group
Corp. ID: 556690-8074
www.truesec.com

Sweden
+ 46 810 00 10
hello@truesec.com

Denmark
+ 46 810 00 10
hello@truesec.com

US
+1 (904) 900-4532
hello@truesec.com

4. Running the decryptor

The decryptor is a wizard-style application. Navigate through the wizard and follow the instructions in the application to recover your files.

Please note that the decryption will take several hours. Do not shutdown the computer until the decryption has completed.

4.1 Setup

Extract the zip archive and run the setup.exe file.

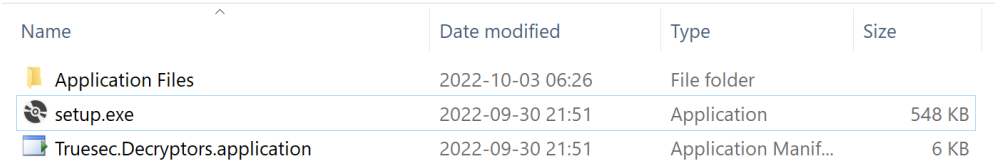


Figure 1 Files in the solution zip archive

The installer is not signed and therefore you will be prompted with the below warning. Click install to continue.

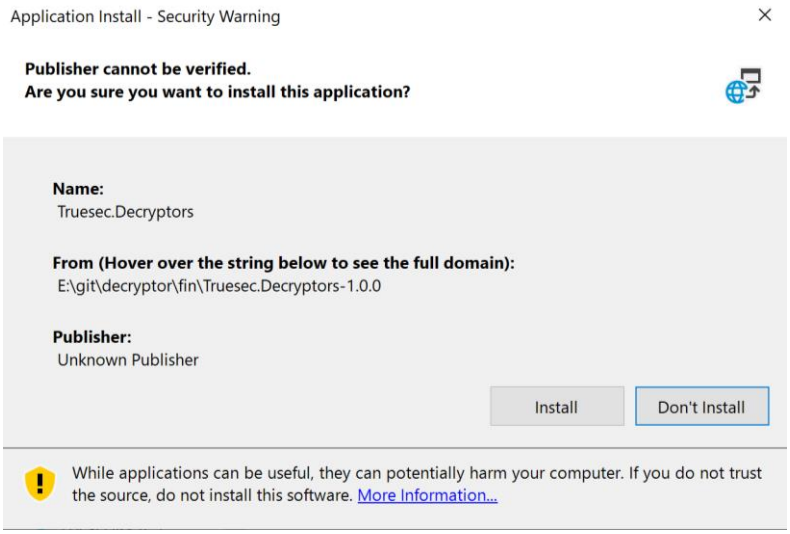


Figure 2 Installation publisher confirmation

When the setup is completed, you should be greeted by the welcome page as seen in the below figure.

Truesec Group
Corp. ID: 556690-8074
www.truesec.com

Sweden
+ 46 810 00 10
hello@truesec.com

Denmark
+ 46 810 00 10
hello@truesec.com

US
+1 (904) 900-4532
hello@truesec.com

Figure 3 Welcome page

4.2 License agreement

Carefully read the license agreement. You must accept the agreement to use this software.

Figure 4 License agreement page

4.3 Settings

Description of configuration options.

Truesec Group
Corp. ID: 556690-8074
www.truesec.com

Sweden
+ 46 810 00 10
hello@truesec.com

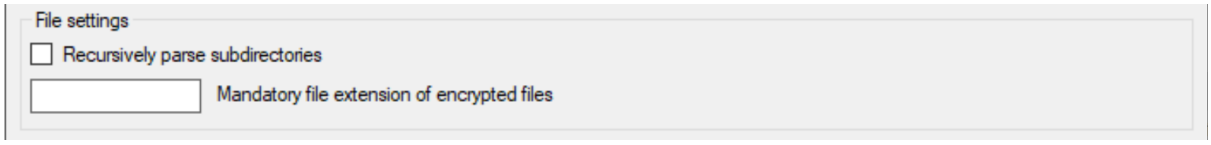
Denmark
+ 46 810 00 10
hello@truesec.com

US
+1 (904) 900-4532
hello@truesec.com

4.3.1 File settings

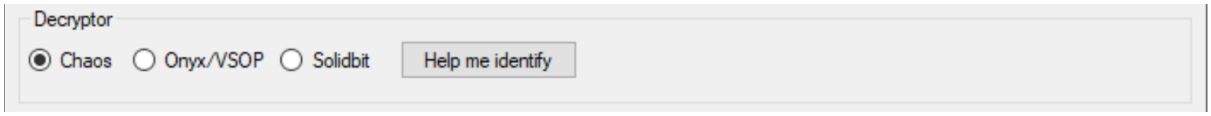
Recursively parse subdirectories – Select the checkbox to recursively parse subfolders for the target folders (selected on the next page in the wizard). If the checkbox is not checked, subdirectories will be skipped.

File extension of encrypted files – Define the extension that was appended to the encrypted files by the ransomware.



4.3.2 Decryptor settings

Decryptor – Select the strain that has encrypted the files you want to decrypt. If you do not know which strain you are affected by, click the "Help me identify" button.



4.3.3 Database settings

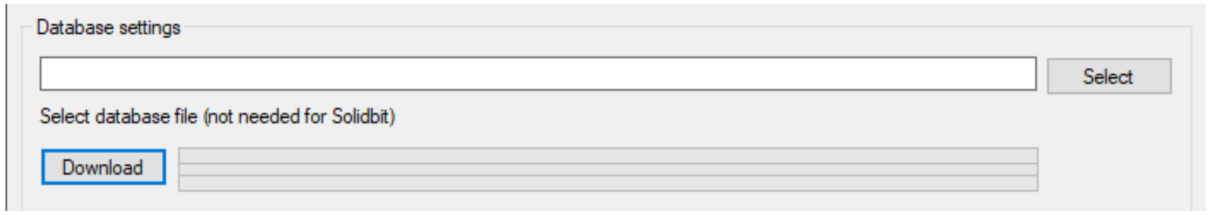
You can either select the database file from your local file system or choose to download the database file. To download the database file your computer must allow outbound 443/HTTPS to Amazon Web Services where the file is hosted.

Note that the database file is 103GB. Please ensure that you have available disk space.

To perform decryption without internet access, please download the file manually from another system with internet access, and then copy the file to your local system. The database file and checksum are available at:

- https://datafile-public.s3.eu-north-1.amazonaws.com/chaos/chaos.db
- https://datafile-public.s3.eu-north-1.amazonaws.com/chaos/chaos_sha1.sum

Optionally, you can also run the database generation script and generate the database to avoid having to wait for the download. Please see the instructions in the Github repository for generating the database.



4.4 Selecting files to decrypt

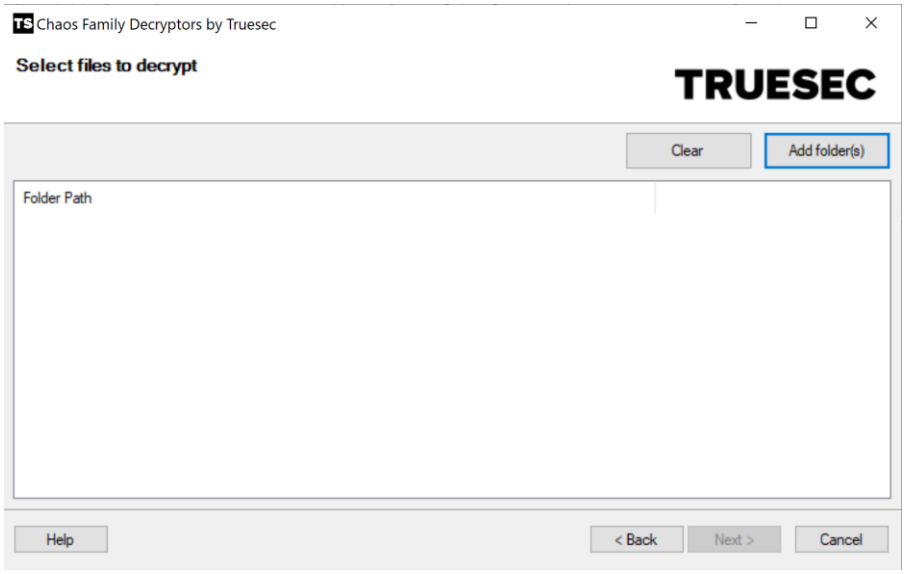
Select the folder(s) containing the files you want to decrypt by clicking the "Add Folder(s)" button.

Truesec Group
Corp. ID: 556690-8074
www.truesec.com

Sweden
+ 46 810 00 10
hello@truesec.com

Denmark
+ 46 810 00 10
hello@truesec.com

US
+1 (904) 900-4532
hello@truesec.com



4.5 Running the decryptor

Please note that the decryption will take several hours. Do not shutdown the computer until the decryption process has completed.

4.6 Verifying and cleanup

After the decryption has completed, your files should be decrypted, and you will be able to access them again.

Please note that the decryptor does not remove any encrypted files. In some cases, the decrypted file will not be valid. Please manually confirm that every decrypted file is valid before removing the encrypted file.

Truesec Group
Corp. ID: 556690-8074
www.truesec.com

Sweden
+ 46 810 00 10
hello@truesec.com

Denmark
+ 46 810 00 10
hello@truesec.com

US
+1 (904) 900-4532
hello@truesec.com