Downloading and Using the Trend Micro Ransomware File Decryptor

Updated: 28 Nov 2016 **Product/Version:** Antivirus+ Security 2016.All , ⊞ **Platform:** Windows 10 32-bit, ⊞

Rating:
485 found this helpful

Category:
Troubleshoot

Solution Id:
1114221

SUMMARY

This guide provides the instructions and location for downloading and using the latest Trend Micro Ransomware File Decryptor tool to attempt to decrypt files encrypted by certain ransomware families.

As an important reminder, the best protection against ransomware is preventing it from ever reaching your system. While Trend Micro is constantly working to update our tools, ransomware writers are also constantly changing their methods and tactics, which can make previous versions of tools such as this one obsolete over time.

Customers are strongly encouraged to continue practicing safe security habits:

1. Make sure you have regular offline or cloud backups of your most important and critical data.
2. Ensure that you are always applying the latest critical updates and patches to your system OS and other key software (e.g. browsers).
3. Install the latest versions of and apply best practice configurations of security solutions such as Trend Micro to provide mutli-layered security.

Trend Micro customers are encouraged to visit the following sites for more information on ransomware and prevention best practices:

Consumer (Home) customers may visit the following site: Consumer (Home) Customers' Guide on Ransomware: Introduction, Prevention and Trend Micro Security Solutions (https://esupport.trendmicro.com/en-us/home/pages/technical-support/1099580.aspx)

Corporate (Business) customers may find additional information and guides here: Corporate (Business) Customers' Guide on Ransomware: Solutions, Best Practice Configuration and Prevention using Trend Micro products (https://success.trendmicro.com/solution/1112223-ransomware-solutions-best-practice-configuration-and-prevention-using-trend-micro-products)

DETAILS

Supported Ransomware Families

The following list describes the known ransomware-encrypted files types can be handled by the latest version of the tool.

Ransomware	File name and extension
CryptXXX V1, V2, V3*	{original file name}.crypt, cryp1, crypz, or 5 hexadecimal characters
CryptXXX V4, V5	{MD5 Hash}.5 hexadecimal characters
Crysis	.{id}.{email address}.xtbl, crypt
TeslaCrypt V1**	{original file name}.ECC
TeslaCrypt V2**	{original file name}.VVV, CCC, ZZZ, AAA, ABC, XYZ
TeslaCrypt V3	{original file name}.XXX or TTT or MP3 or MICRO
TeslaCrypt V4	File name and extension are unchanged

TeslaCrypt V4	File name and extension are unchanged
SNSLocker	{Original file name}.RSNSLocked
AutoLocky	{Original file name}.locky
BadBlock	{Original file name}
777	{Original file name}.777
XORIST	{Original file name}.xorist or random extension
XORBAT	{Original file name}.crypted
CERBER V1	{10 random characters}.cerber
Stampado	{Original file name}.locked
Nemucod	{Original file name}.crypted
Chimera	{Original file name}.crypt
LECHIFFRE	{Original file name}.LeChiffre
MirCop	Lock.{Original file name}
Jigsaw	{Original file name}.random extension
Globe/Purge	V1: {Original file name}.purge V2: {Original file name}.{email address + random characters} V3: Extension not fixed or file name encrypted
DXXD	V1: {Original file name}.{Original extension}dxxd
Teamxrat/Xpan	V2: {Original filename}.__xratteamLucked
Crysis	.{id}.{email address}.xtbl, crypt

ℹ * - CryptXXX V3 decryption may not recover the entire file (partial data decryption). Please see the section titled **Important Note about Decrypting CryptXXX V3** below.

** - Users will need to contact Trend Micro technical Support to request the separate tool TeslacryptDecryptor 1.0.xxxx MUI for TeslaCrypt V1 and V2 files. Both tools support V3 and V4.

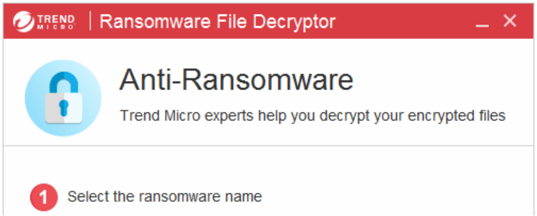
Obtaining and Executing the Tool(s)

1. Click the **Download** button below to obtain the latest version of the Trend Micro Ransomware File Decryptor tool. Decompress (unzip) and then launch either the included RansomwareFileDecryptor exe file.

   Download RansomwareFileDecryptor (http://solutionfile.trendmicro.com/SolutionFile/EN-1114221/RansomwareFileDecryptor%201.0.1654%20MUI.zip)

2. Upon launch, users will be required to accept the End User License Agreement (EULA) to proceed.

3. After accepting the EULA, the tool will proceed to the main user interface (UI). From here, users will be presented with a step-by-step guide to perform the file decryption.

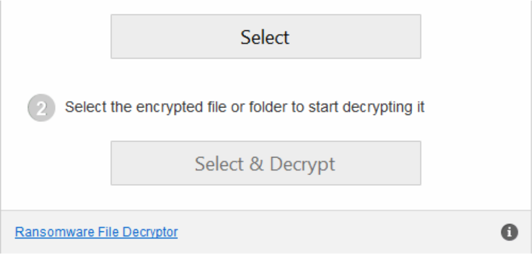


TREND MICRO | Ransomware File Decryptor

Anti-Ransomware

Trend Micro experts help you decrypt your encrypted files

1 Select the ransomware name

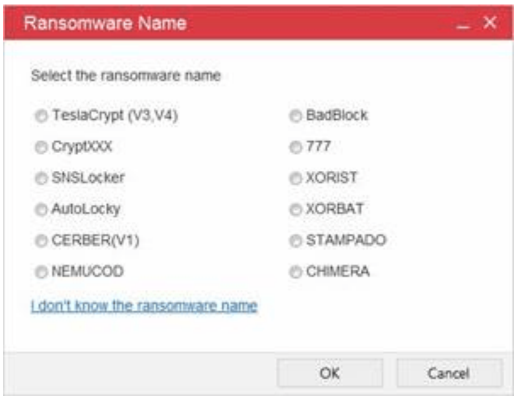

Select
2 Select the encrypted file or folder to start decrypting it
Select & Decrypt
Ransomware File Decryptor

COLLAPSE ALL

Detailed Steps

Step 1: Select the ransomware name

Most ransomware usually includes a text file or html file to inform the user that his/her system has been infected by a certain type of ransomware. Using this information, an affected user can select the suspected ransomware name to decrypt files. Users having trouble identifying the type of ransomware should contact Trend Micro Technical Support for further assistance.


Ransomware Name

Select the ransomware name

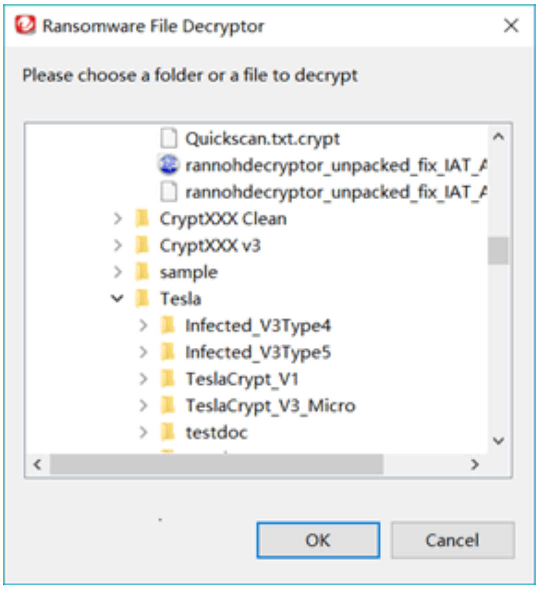
○ TeslaCrypt (V3,V4)
○ CryptXXX
○ SNSLocker
○ AutoLocky
○ CERBER(V1)
○ NEMUCOD
○ BadBlock
○ 777
○ XORIST
○ XORBAT
○ STAMPADO
○ CHIMERA

I don't know the ransomware name

*Note: When selecting the "**I don't know the ransomware name**" option, the tool will prompt the user to select a target file to be decrypted and will try and automatically identify the ransomware based on the file signature.*

Step 2: Select the encrypted file or folder

The tool can either attempt to decrypt a single file or all files in a folder and its sub-folders by using recursive mode. By clicking “Select & Decrypt”, choose a folder or a file and click **OK** to start the decrypting process.

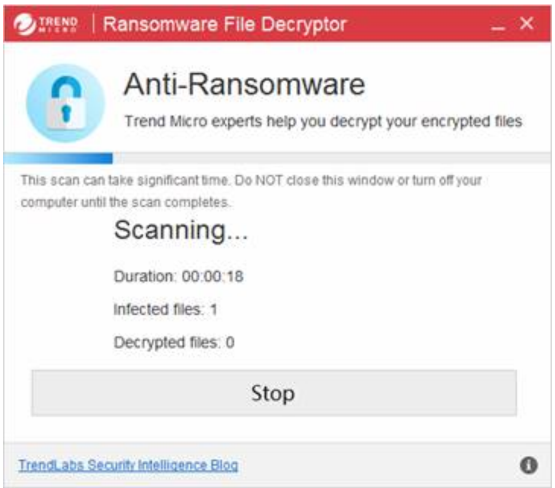

Ransomware File Decryptor

Please choose a folder or a file to decrypt

Quickscan.txt.crypt
rannohdecryptor_unpacked_fix_IAT_A
rannohdecryptor_unpacked_fix_IAT_A
CryptXXX Clean
CryptXXX v3
sample
Tesla
Infected_V3Type4
Infected_V3Type5
TeslaCrypt_V1
TeslaCrypt_V3_Micro
testdoc

Step 3: Start decrypting files

After the file(s) or folder(s) are selected, the tool will start scanning and decrypting files automatically.



Ransomware File Decryptor

Anti-Ransomware

Trend Micro experts help you decrypt your encrypted files

This scan can take significant time. Do NOT close this window or turn off your computer until the scan completes.

Scanning...

Duration: 00:00:18

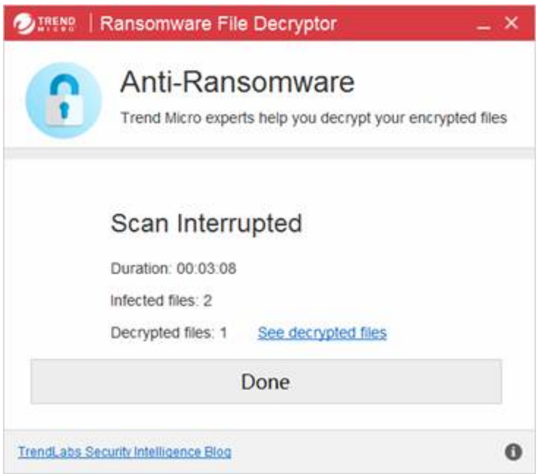
Infected files: 1

Decrypted files: 0

If the scan target is a folder, the tool will collect some file information from the target folder first to help identify which files need to be decrypted. During the scan, a scrollbar will indicate the decrypting progress, and the UI will be updated to indicate how many files are encrypted and the number of files have been decrypted.

The tool can decrypt certain types of ransomware-encrypted files (e.g. TeslaCrypt) files very quickly. However, other file types (e.g. CryptXXX) may take significantly longer. The overall duration also depends on how many files are located in the target folder.

If **Stop** is clicked during scanning, the process will be interrupted.



Ransomware File Decryptor

Anti-Ransomware

Trend Micro experts help you decrypt your encrypted files

Scan Interrupted

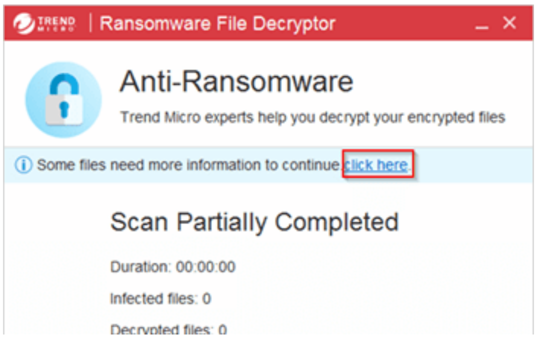
Duration: 00:03:08

Infected files: 2

Decrypted files: 1 See decrypted files

Step 4: Decrypting CyptXXX V1, XORIST, XORBAT or Nemucod (optional)

If the tool identifies files encrypted by CryptXXX V1 ransomware, it will ask the user to provide additional information to proceed due to some unique processing required for the specific decryption.



Ransomware File Decryptor

Anti-Ransomware

Trend Micro experts help you decrypt your encrypted files

Some files need more information to continue click here

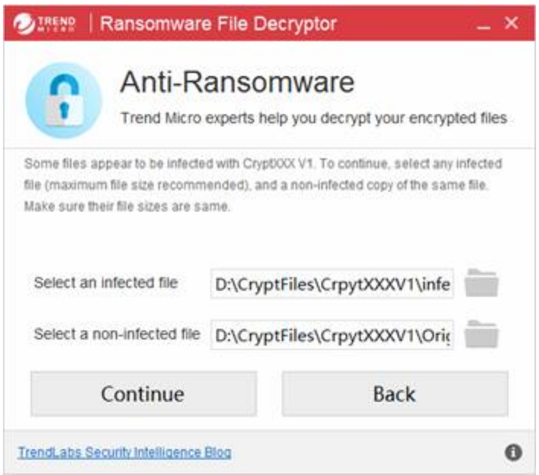
Scan Partially Completed

Duration: 00:00:00

Infected files: 0

Decrypted files: 0

After selecting the “click here” option highlighted above, another dialog will appear asking for a file pair. The user will need to select a infected file and a matching non-infected file if there is an available backup copy (the larger the file size the better).


Ransomware File Decryptor
Anti-Ransomware
Trend Micro experts help you decrypt your encrypted files

Some files appear to be infected with CryptXXX V1. To continue, select any infected file (maximum file size recommended), and a non-infected copy of the same file. Make sure their file sizes are same.

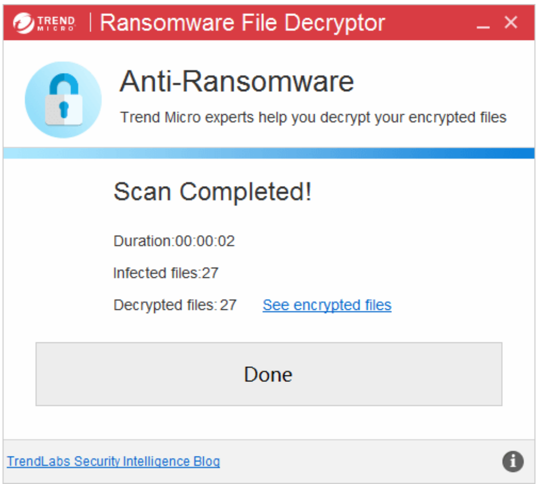
Select an infected file: D:\CryptFiles\CrpytXXXV1\infe

Select a non-infected file: D:\CryptFiles\CrpytXXXV1\Oriç

Continue
Back
TrendLabs Security Intelligence Blog

Step 5: Finish decrypting files

Once the scan and decryption process is finished, the UI will show the results.


Ransomware File Decryptor
Anti-Ransomware
Trend Micro experts help you decrypt your encrypted files

Scan Completed!

Duration:00:00:02

Infected files:27

Decrypted files: 27

See encrypted files
Done
TrendLabs Security Intelligence Blog

By clicking **See encrypted files**, the tool opens the encrypted file location or folder which was selected for scanning. The decrypted files are resident in opened folder.

The decrypted file name(s) will be the same as the previously encrypted file(s), with the exception being the removal of the extension appended by the ransomware.

For those file(s) encrypted without the file name changing, the decrypted file name will be {original file name} decrypted.{extension}.

By clicking **Done**, the tool returns to the main UI. Repeat step 1 and 2 to decrypt more files.

Important Note about Decrypting CryptXXX V3

Decrypting BadBlock

CERBER Decryption Limitations

CERBER Decryption Limitations

Obtaining Tool Logs

Video How-to

Notes and Limitations

File Verification and Checksums

FEEDBACK

Did this article help you? Yes No

NEED MORE HELP?

Create a technical support case (/new-request) if you need further support.

(/TS_Portal_ImproveExperienceModal)

Contact Support (/contact-support-europe)

Download Center (http://downloadcenter.trendmicro.com/)

Product Documentation (http://docs.trendmicro.com/en-us/home.aspx)

Support Policies (/support-policies)

Product Vulnerability (/vulnerability-response)

Feedback (/survey/solution/1114221

Europe

TREND (http://www.trendmicro.com/)

Business Support Home (/business-support) • Legal Policies & Privacy (http://www.trendmicro.com/us/about-us/legal-policies/index.html) • Site Map (/sitemap)

- FAQ (/faq)