

# Shade / Troldeh Ransomware decryption tool

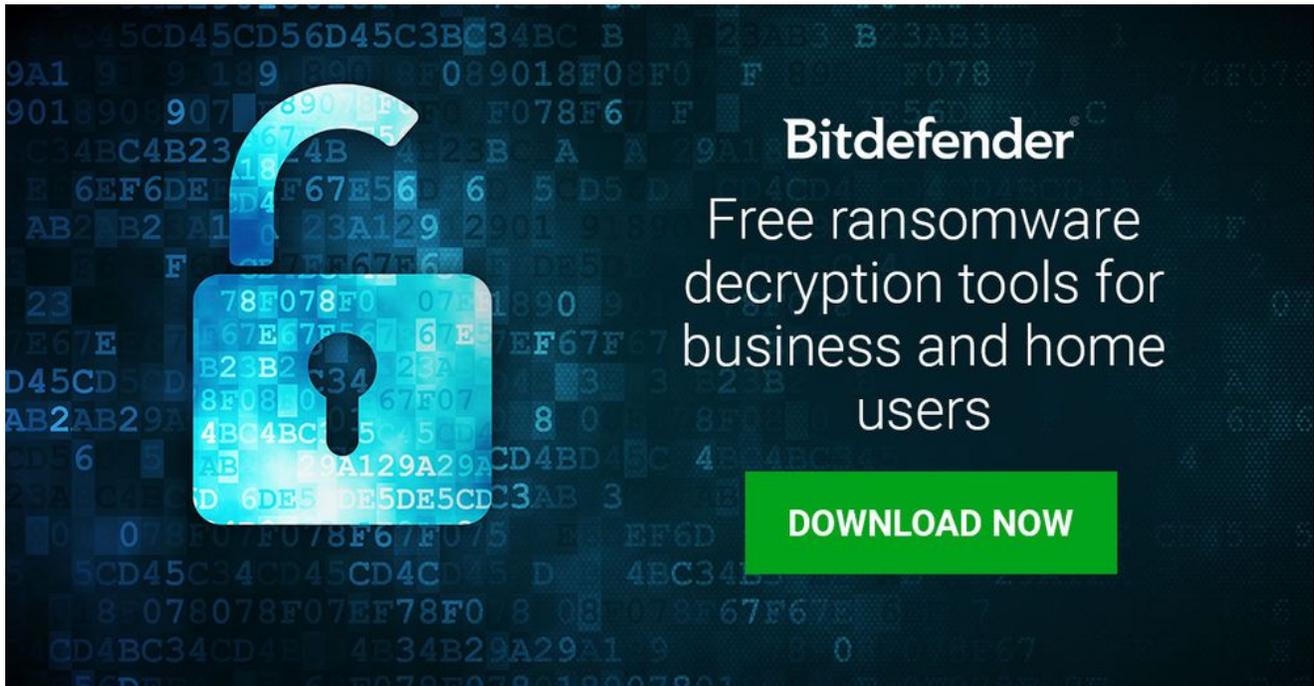
---

**B** [labs.bitdefender.com/2020/05/shade-troldesh-ransomware-decryption-tool/](https://labs.bitdefender.com/2020/05/shade-troldesh-ransomware-decryption-tool/)

The image shows the Bitdefender logo in white text on a black background. The word "Bitdefender" is written in a bold, sans-serif font, with a registered trademark symbol (®) to the upper right of the letter 'r'.

Bitdefender  
May 02, 2020

One product to protect all your devices, without slowing them down.  
[Free 90-day trial](#)



We have just released an updated decryption tool for Shade (Troidesh) Ransomware. As a long-established family of ransomware, Shade has been in operation since 2014, and has been operating consistently ever since.

In late April 2020, its operators announced that they are stopping the Shade operation and publicly released around 750,000 decryption keys hinting that cyber-security companies should build a better decryptor than theirs.

### **TL;DR, just show me the download**

You can download the decryptor here to get your files back for free.

[mks\_button size="large" title="Download the Shade Ransomware decryption tool" style="squared" url="https://labs.bitdefender.com/wp-content/uploads/downloads/shade-troidesh-decryption-tool/" target="\_self" bg\_color="#81d742" txt\_color="#FFFFFF" icon="" icon\_type="" nofollow="0"]

If you are interested in how the tool works, we have more information below.

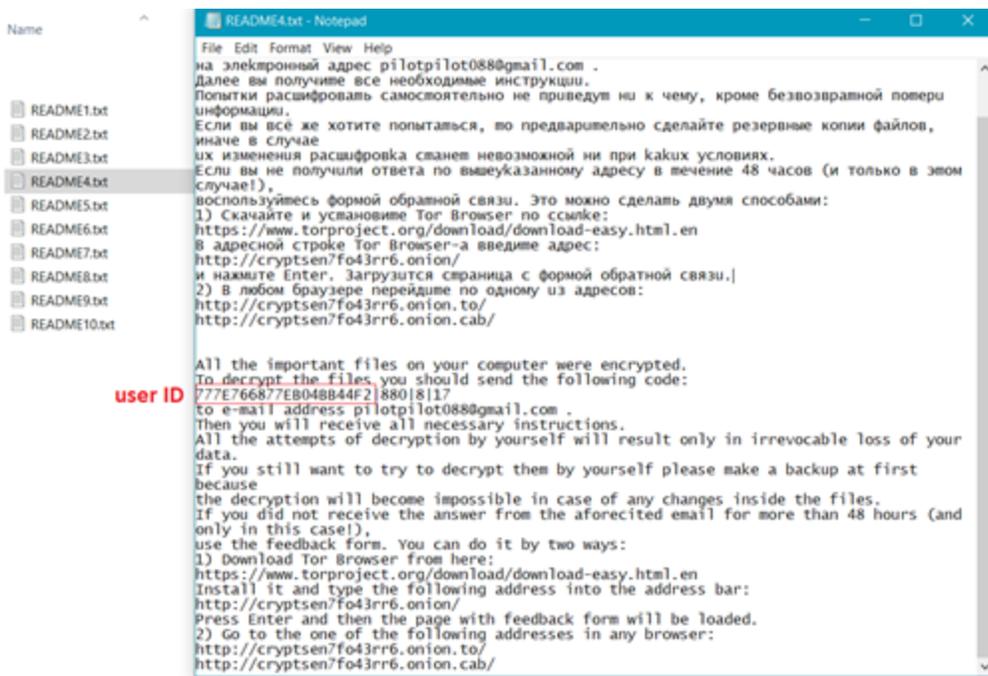
### **Technical description:**

This tool recovers files encrypted by Shade/Troidesh ransomware. While it might be easy for the untrained eye to mistake it with Crisis/Dharma ransomware, Shade is quite different in several ways. One can tell this ransomware family and version apart by the extension it appends to the encrypted files, by some 10 similar ransom-notes or by the way encrypted files are named (base64):

Extensions used for encrypted file names:

.xtbl  
 .ytbl  
 .breaking\_bad  
 .heisenberg  
 .better\_call\_saul  
 .los\_pollos  
 .da\_vinci\_code  
 .magic\_software\_syndicate  
 .windows10  
 .windows8  
 .no\_more\_ransom  
 .tyson  
 .crypted000007  
 .crypted000078  
 .rsa3072  
 .decrypt\_it  
 .dexter  
 .miami\_california

Ransom-notes:



User Ids, required for key match, are also found in encrypted file names, for most ransomware sub-versions. For older versions of the malware, the ID can be recovered from ransom-notes, or by brute-forcing the limited set of released keys.

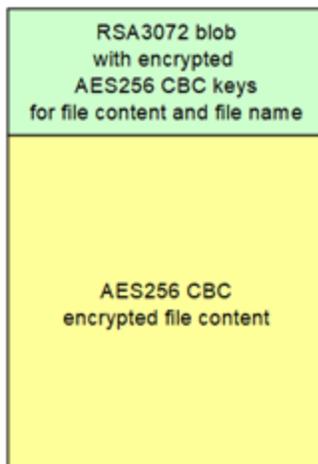
Name	Date modified	Type	Size
ajeRCMncOPf497VPB8YCwupm7deM6Cn18C6bYy9fk=777E766877E8048B44F2_crypted000007	5/1/2020 1:08 PM	CRYPTED000007 FL..	35,805 KB
mR8-RqCNjEms0simbd5QWUPID-Kosojd817Uogp2A=.xtbl ?	5/1/2020 3:41 PM	XTBL File	9,934 KB
Q5741PMpWHLs1b9UzkaMVv80awqvw5Q3Dq8LoCM8oEj--Lpf9VAUztfmCQ2ADCE13159308E7EBAD1da_vinci_code	5/1/2020 5:36 PM	DA_VINCL_CODE FL..	6,801 KB
TRuk+shZABJUTjwhjOZZ-4TdnjWe4bW6XP3AFTyNpHKTeBhA8DXSgmmc1DwoKN.378001C79080C7AC5BCB_crypted000007	5/1/2020 2:40 PM	CRYPTED000007 FL..	1,622 KB
VWnbWdwOSmr9WmmNn2FWeSfBDG6NeQP6Idig-rVli=@A1ACEAAEB353168EBDFda_vinci_code	5/1/2020 3:18 PM	DA_VINCL_CODE FL..	36,857 KB
VfgBL6teNR2ARyP8JhrzADEpMp9PMNURbswXIOE=D0D29D15EA056F5C9496.xtbl	5/1/2020 4:47 PM	XTBL File	536 KB

By default malware comes with some public RSA3072 keys, which are used to encrypt files, if no server responds within several hours. The authors released the entire set of encryption keys used in all malware versions in a public Github repository.

While victims whose systems could successfully connect to server would have custom encryption keys, those who got infected with no active connection would have been encrypted by hardcoded RSA public keys.

The set of dynamic generated keys and uploaded to ransomware owner servers take up to 1.8GB (~749K), the static shipped private keys are only 1.6K in size, and do not exceed 4MB.

Our decryption tool is able to identify on the fly corresponding keys, cache them, and apply faster on subsequent decryption attempts. The tool does not require any additional input from the user in order to decrypt. It requires an active internet connection to compute the dynamic keys, should files have been infected in online mode.



## How to use this tool

**Step 1:** Download the decryption tool below and save it on your computer.

[Download the Shade decryptor](#)

*Note: This tool **REQUIRES** an active internet connection, as our servers will attempt to reply the submitted ID with a possible valid RSA-3072 private key. If this step succeeds, the decryption process will continue.*

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

**Step 3:** Agree to the End User License Agreement

# License Agreement

Please read and confirm if you agree.



Subscription Agreement and Terms of services for Home User Solutions NOTICE TO ALL USERS: PLEASE READ THIS AGREEMENT CAREFULLY! BY OPENING THIS PACKAGE, BREAKING THE SEAL, BY SELECTING "I ACCEPT", "OK", "CONTINUE", "YES" OR BY INSTALLING OR USING THE SOFTWARE IN ANY WAY, YOU ARE INDICATING YOUR COMPLETE UNDERSTANDING AND ACCEPTANCE OF THE TERMS OF THIS AGREEMENT. If the Software is downloaded from the websites (for paid or trial use purposes), this Agreement will be accepted and a contract formed when the end user ("You") selects an "I Accept", "OK" or "Yes" button or box below prior to download or installation. The Agreement is made available on Bitdefender websites as well for your reference. Certain Bitdefender Solution may require an active and stable connection to the Internet in order to function. It is therefore your responsibility to ensure that you have at all times an active and stable Internet connection. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS DO NOT INSTALL OR ACCESS THE SOFTWARE OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE, AND CONTACT YOUR VENDOR OR CUSTOMER SERVICE, FOR INFORMATION ON HOW TO OBTAIN A REFUND OF THE MONEY YOU PAID FOR THE SOFTWARE AT ANY TIME DURING THE THIRTY (30) DAYS PERIOD FOLLOWING THE DATE OF PURCHASE. SOLUTION REGISTRATION. By accepting this Agreement. You agree to register

I agree with the terms of use

CONTINUE

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

If you encounter any issues, please contact us via the e-mail address specified inside the tool.

If you checked the backup option, you will have both the encrypted and decrypted files at the end of the process. You may 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 in bulk. We do not encourage you to do this, until you double-check your files can be opened safely and there is no trace of damage.

**Do not remove large files, as their decryption may be tricky, and we may have some updates for specific cases where decryption may have failed.**

## Acknowledgement:

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

## TAGS

**AUTHOR**

---

---



hical  
p eye.”