Shade / Troldesh Ransomware decryption tool

labs.bitdefender.com/2020/05/shade-troldesh-ransomware-decryption-tool/

Bitdefender
May 02, 2020

We have just released an updated decryption tool for Shade (Troldesh) 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-troldesh-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.

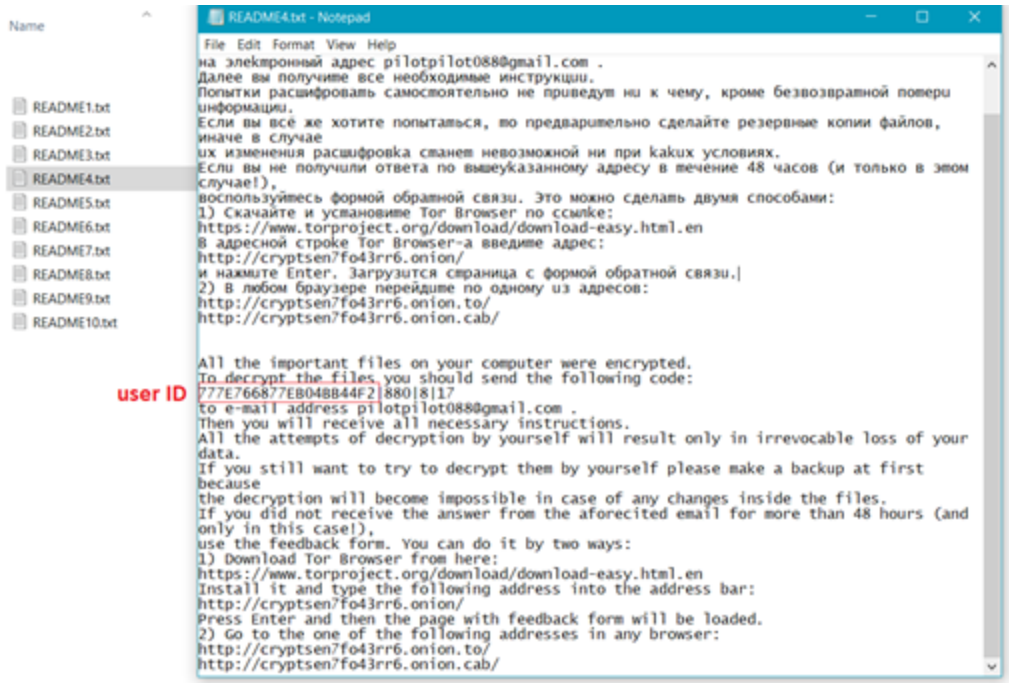
Technical description:

This tool recovers files encrypted by Shade/Troldesh ransomware. While it might be easy for the untrained eye to mistake it with Crysis/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:



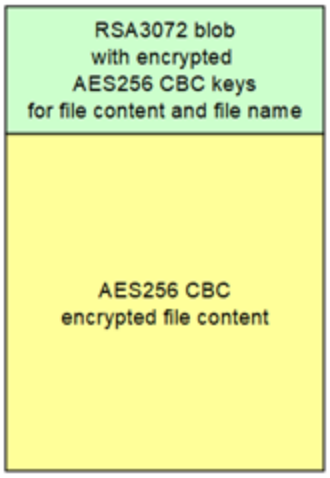
User Ids, required for key match, are also found in encrypted file names, for most ransomware sub-versions. For older versions of the malware, the ID can be recovered from ransom-notes, or by brute-forcing the limited set of released keys.

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 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

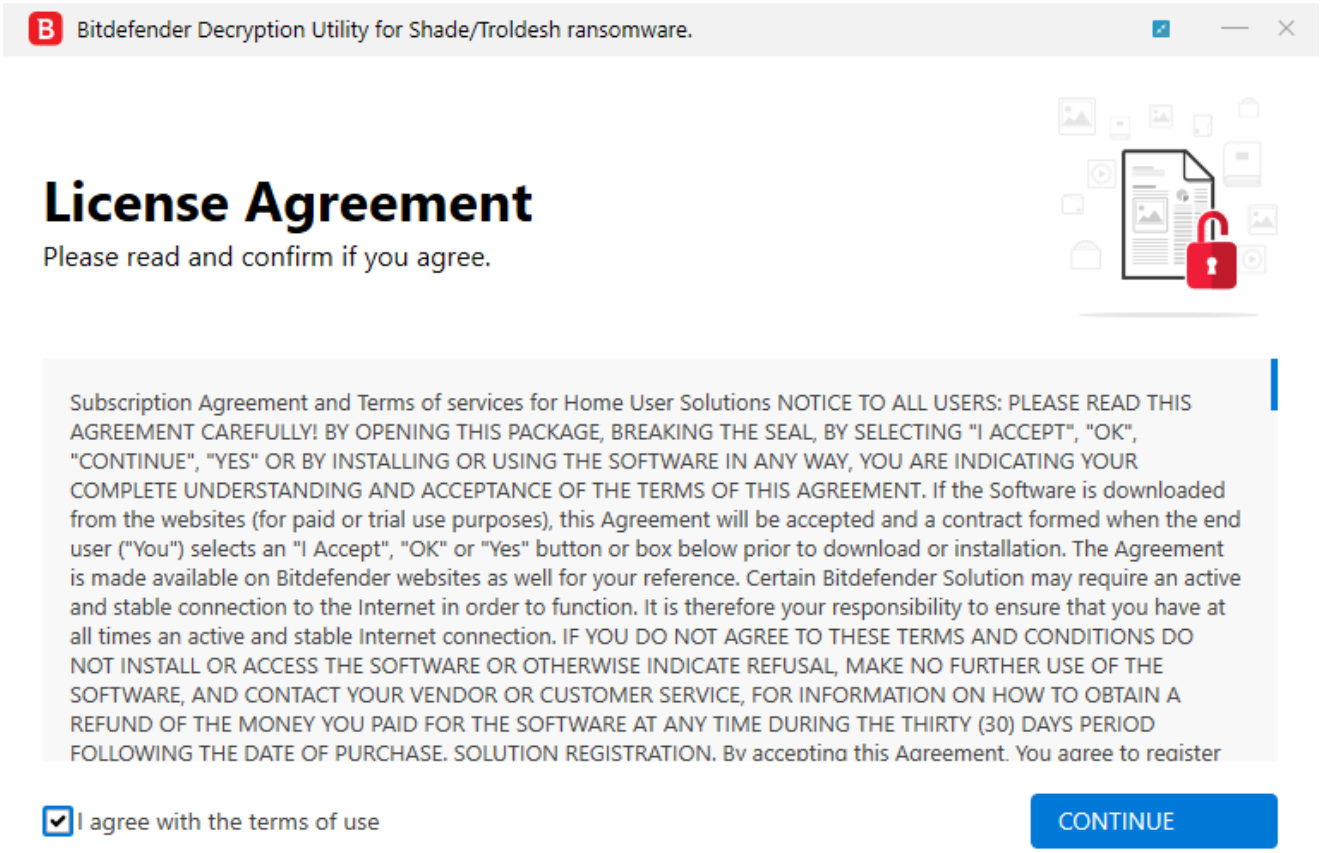
Step 1: Download the decryption tool below and save it on your computer.

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 BDParadiseDecryptor.exe) and allow it to run by clicking Yes in the UAC prompt.

Step 3: Agree to the End User License Agreement



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

anti-malware research free tools

AUTHOR

hical
p eye.”