Paradise Ransomware decryption tool

labs.bitdefender.com/2020/01/paradise-ransomware-decryption-tool

Bitdefender

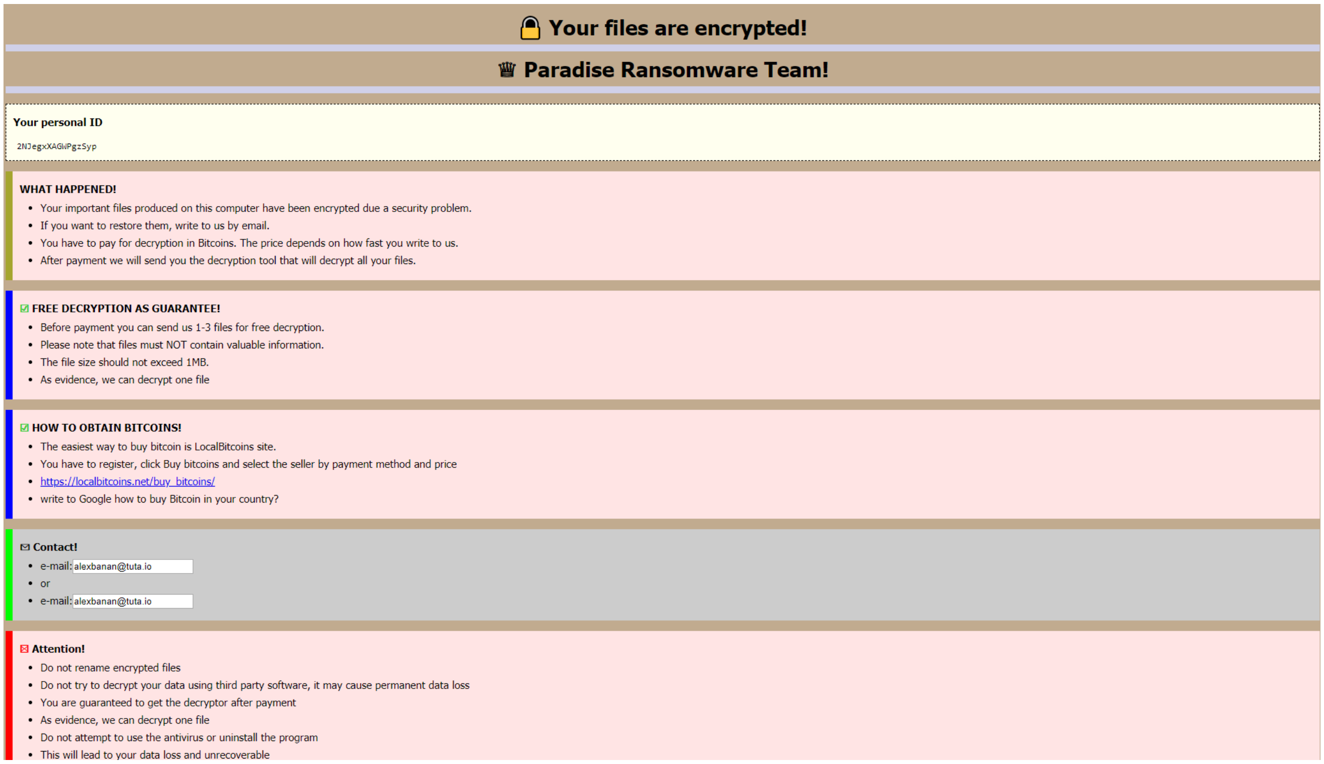
January 16, 2020

Bitdefender
Free ransomware decryption tools for business and home users
DOWNLOAD NOW

We’re happy to announce a new decryptor for Paradise Ransomware.

Paradise Ransomware, initially spotted in 2017, has been aggressively marketed as a service to interested affiliates. After infection, it checks whether the keyboard language is set to Russian, Kazakh, Belarus or Ukrainian and, if so, exits without encrypting. Otherwise, it encrypts files and deletes shadow copies to prevent the user from restoring them.

After encryption, it displays a ransom message:



🔒 **Your files are encrypted!**

♛ **Paradise Ransomware Team!**

Your personal ID

2NJegxXAGWPgzSyp

WHAT HAPPENED!

- Your important files produced on this computer have been encrypted due a security problem.
- If you want to restore them, write to us by email.
- You have to pay for decryption in Bitcoins. The price depends on how fast you write to us.
- After payment we will send you the decryption tool that will decrypt all your files.

☑ **FREE DECRYPTION AS GUARANTEE!**

- Before payment you can send us 1-3 files for free decryption.
- Please note that files must NOT contain valuable information.
- The file size should not exceed 1MB.
- As evidence, we can decrypt one file

☑ **HOW TO OBTAIN BITCOINS!**

- The easiest way to buy bitcoin is LocalBitcoins site.
- You have to register, click Buy bitcoins and select the seller by payment method and price
- https://localbitcoins.net/buy_bitcoins/
- write to Google how to buy Bitcoin in your country?

✉ **Contact!**

- e-mail: alexbanan@tuta.io
- or
- e-mail: alexbanan@tuta.io

☒ **Attention!**

- Do not rename encrypted files
- Do not try to decrypt your data using third party software, it may cause permanent data loss
- You are guaranteed to get the decryptor after payment
- As evidence, we can decrypt one file
- Do not attempt to use the antivirus or uninstall the program
- This will lead to your data loss and unrecoverable

The new Bitdefender decryptor can restore the following file extensions:

. FC, . 2ksys19, . p3rf0rm4, . Recognizer, . VACv2, . paradise, . CORP, .immortal, . exploit, . prt, . STUB, . sev, . sambo

How to use this tool

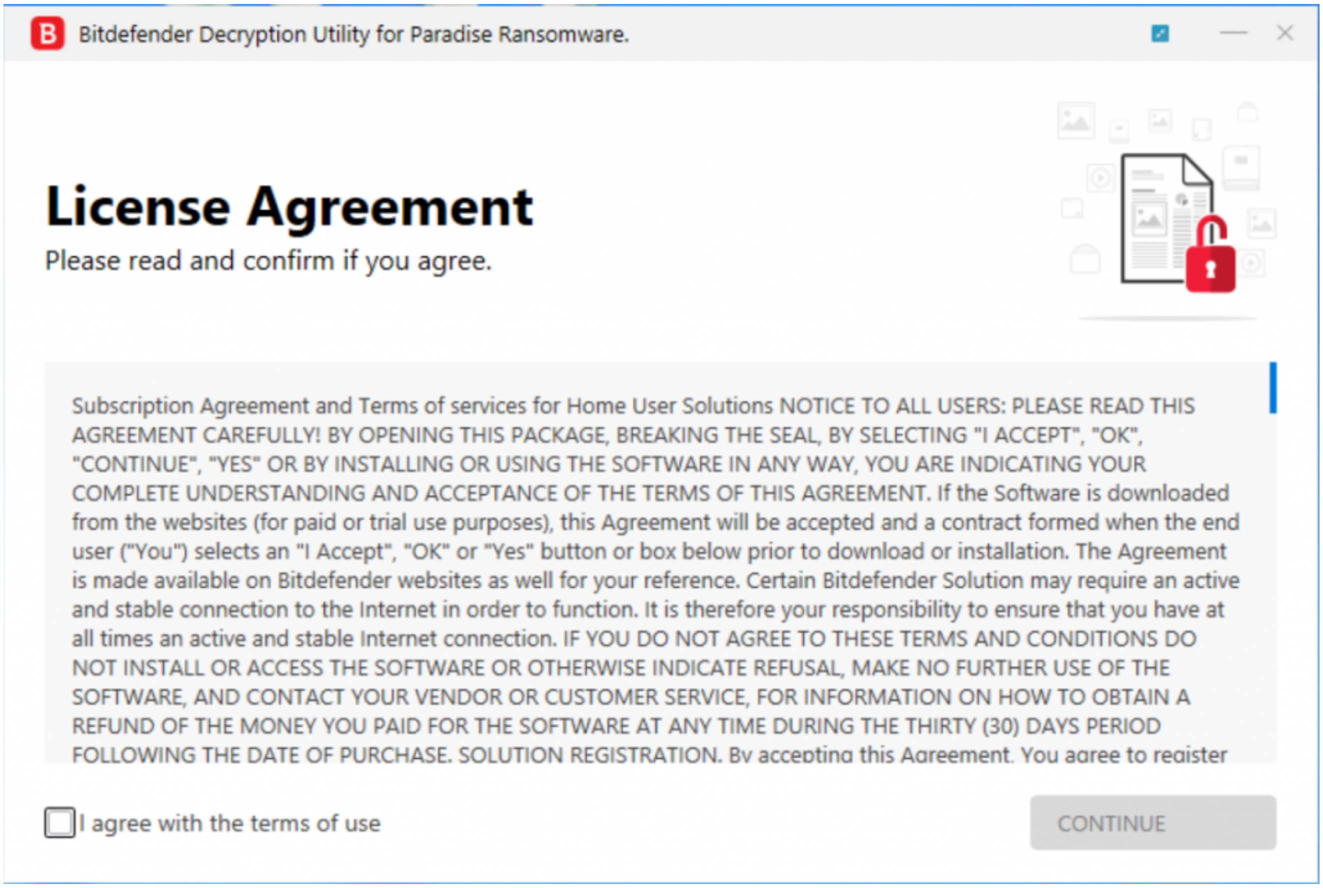
Step 1: Download the decryption tool below and save it on your computer.

Download the Paradise decryptor

Note: This tool does not require an active internet connection.

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



Bitdefender Decryption Utility for Paradise Ransomware.

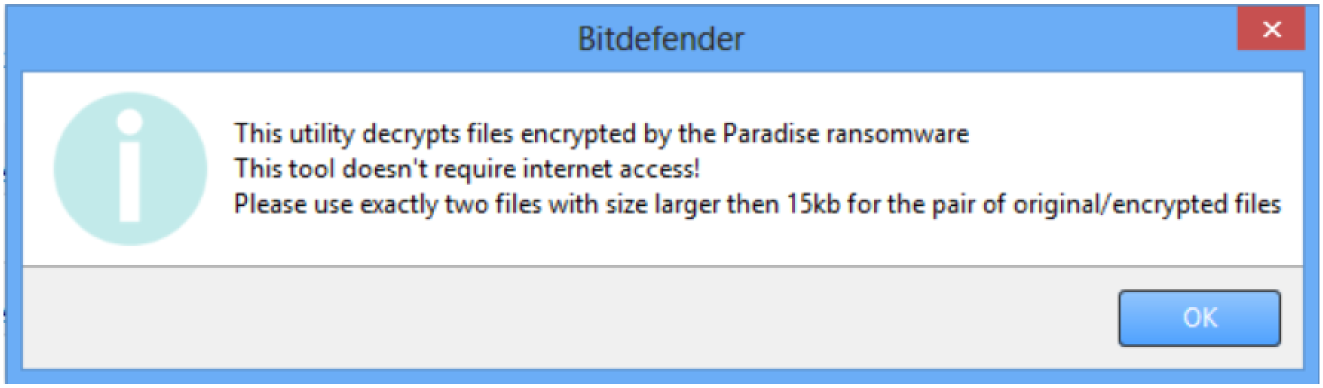
License Agreement

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

We strongly recommend you also select “Backup files” before starting the decryption process, in case anything occurs while decrypting. Then press “Scan”.

The “test folder” must contain a pair of original/encrypted files, which will be used to determine the decryption key. It is essential that this folder only contain **a pair of original and encrypted files** and both files should be at least 15 kb in size.



This utility decrypts files encrypted by the Paradise ransomware
This tool doesn't require internet access!
Please use exactly two files with size larger then 15kb for the pair of original/encrypted files

Users may also check the "Overwrite existing clean files" option under "Advanced options" so the tool will overwrite possible clean files present with their decrypted equivalent.

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

If you encounter any issues, please contact us at forensics@bitdefender.com.

If you checked the backup option, you will see both the encrypted and decrypted files. You can also find a log describing the decryption process, in **%temp%\BDRemovalTool** folder:

To get rid of your encrypted files after decryption, just search for files matching the extension and remove them in bulk. We do not encourage you to do this, unless you have double-checked that your files can be opened safely and none of the decrypted files are damaged.

Silent execution (via cmdline)

The tool can also be executed silently via a command line. If you need to automate deployment of the tool inside a large network, you might want to use this feature.

> **-help** – provides information on how to run the tool silently (this information will be written in the log file, not on console)

- **start** - this argument allows the tool to run silently (no GUI)
- –**path** - this argument specifies the path to scan
- –**test** - this argument specifies the test path to a pair of original/encrypted files
- **o0:1** - enables **Scan entire system** option (ignoring **-path** argument)
- **o1:1** - enables **Backup files** option
- **o2:1** - enables **Overwrite existing files** option

Examples:

BDParadiseDecryptor.exe start -path:"C:\" -> the tool will start with no GUI and scan **C:\**

BDParadiseDecryptor.exe start o0:1 -> the tool will start with no GUI and scan the entire system

BDParadiseDecryptor.exe start o0:1 o1:1 o2:1 -> the tool will scan the entire system, backup encrypted files and overwrite present clean files

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

Bitdefender

The meaning of Bitdefender’s mascot, the Dacian Draco, a symbol that depicts a mythical animal with a wolf’s head and a dragon’s body, is “to watch” and to “guard with a sharp eye.”

View all posts

Bitdefender®