Fonix Ransomware Decryptor

B labs.bitdefender.com/2021/02/fonix-ransomware-decryptor/



Bogdan BOTEZATU February 04, 2021

One product to protect all your devices, without slowing them down. <u>Free 90-day trial</u>



A decryptor for Fonix Ransowmare is now available for download. Also known as FonixCrypter or Xinof, this family of malware was initially spotted in June 2020 and went out of business in late January this year. The news, broken by one of the project's administrators, also includes master keys and a bare-bones decryptor that can potentially be used to recover one file at a time.

Bitdefender researchers have been working on a free decryptor that can safely help victims get back their ransomed information for free.

The tool works on an infected PC with an active internet connection.

How to use this tool

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

Download the Fonix decryptor

Step 2: Double-click the file (previously saved as BDFonixDecryptor.exe) and allow it to run.





B Bitdefender Decryption Utility for Fonix ransomware.	• - ×
License Agreement Please read and confirm if you agree.	
Subscription Agreement and Terms of services for Home User Solutions NOTICE TO ALL USERS: PL AGREEMENT CAREFULLYI BY OPENING THIS PACKAGE, BREAKING THE SEAL, BY SELECTING 'I ACC 'CONTINUE', 'YES' OR BY INSTALLING OR USING THE SOFTWARE IN ANY WAY, YOU ARE INDICA COMPLETE UNDERSTANDING AND ACCEPTANCE OF THE TERMS OF THIS AGREEMENT. If the Soft from the websites (for paid or trial use purposes), this Agreement will be accepted and a contract user ('You') selects an 'I Accept', 'OK' or 'Yes' button or box below prior to download or installat is made available on Bitdefender websites as well for your reference. Certain Bitdefender Solution and stable connection to the Internet in order to function. It is therefore your responsibility to ens all times an active and stable Internet connection. IF YOU DO NOT AGREE TO THESE TERMS AND O NOT INSTALL OR ACCESS THE SOFTWARE OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHE SOFTWARE, AND CONTACT YOUR VENDOR OR CUSTOMER SERVICE, FOR INFORMATION ON HO REFUND OF THE MONEY YOU PAID FOR THE SOFTWARE AT ANY TIME DURING THE THIRTY (30)	LEASE READ THIS "EPT", "OK", TING YOUR tware is downloaded formed when the end tion. The Agreement may require an active ure that you have at CONDITIONS DO R USE OF THE W TO OBTAIN A DAYS PERIOD
I agree with the terms of use	CONTINUE

Note: The tool requires that affected users must have at least 1 cpriv.key file present on their PCs, either in the target folder to decrypt, or anywhere else on disk(s).

Step 4: Select "Scan Entire System" if you want to search for all encrypted files, or just add the path to the location you previously saved the encrypted files in.

B Bitdefender Decryption Utility for Fonix ransomware.	- ×
Get the best ransomware protection Bitdefender 2019 intercepts any kind of ransomware attack.	Bitdefender
Please enter the necessary information to start	
Scan entire system	
Backup files	
Select the encrypted folder	
[FULL SYSTEM]	BROWSE
START TO	OOL ADVANCED OPTIONS

We strongly recommend that you also select "Backup files" before starting the decryption process should issues occur while decrypting. Then press "Start Tool".

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

To remove the encrypted files left behind, you should search for files matching the extension and mass-remove them. We do not encourage you to do this until you made sure that your files can be opened safely and there is no damage to the decrypted files.

Acknowledgement:

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

TAGS

anti-malware research free tools



hood at @Bitdefender as director of