# Fonix Ransomware Decryptor



Bogdan BOTEZATU
February 04, 2021


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.

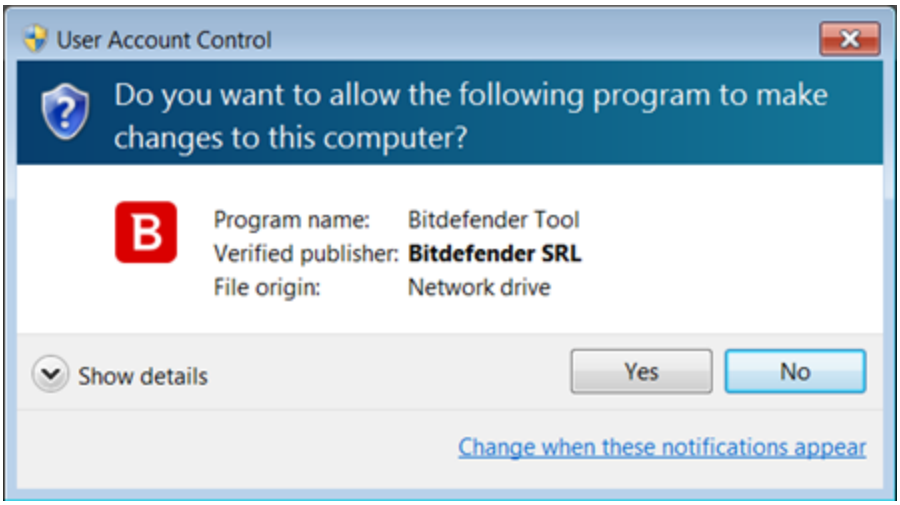
*The tool works on an infected PC with an active internet connection*.

How to use this tool

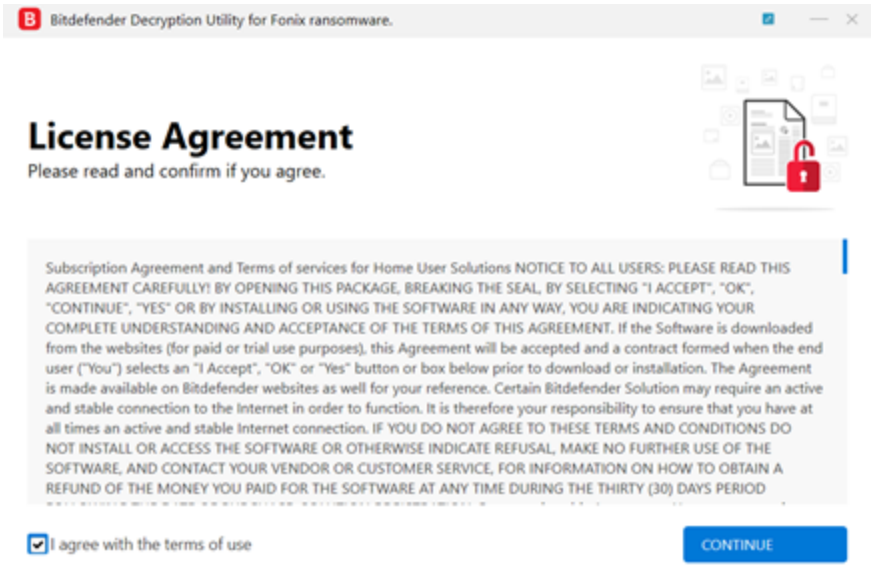
**Step 1**: Download the decryption tool below and save it on your computer.

Download the Fonix decryptor

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

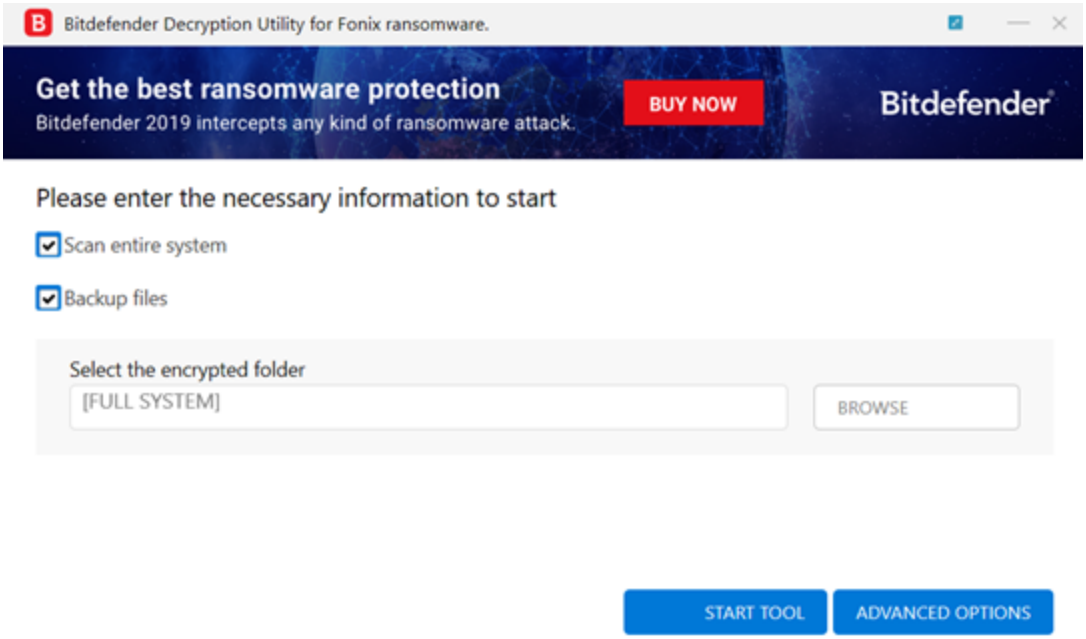



**Step 3**: Select “I Agree” in the License Agreement screen




**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.




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 (http://www.openssl.org/)

## TAGS

anti-malware research  free tools

## AUTHOR

hood at @Bitdefender as director of