

## **FONIX Ransomware Decryption Tool**

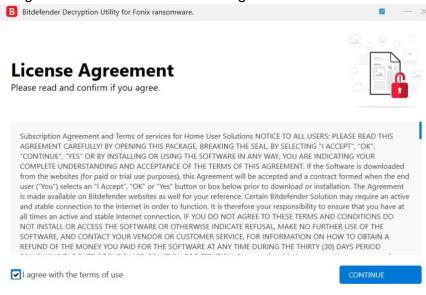
**Step 1:** Download the decryption tool and save it somewhere in your computer from: <u>download.bitdefender.com/am/malware\_removal/BDFONIXDecryptor.exe</u> *This tool works on an infected pc that has an active internet connection.* 

The tool is able to decrypt at least the ransomware versions: **4.4.x**, **4.3.x**, **4.2.x**, **3.x** These versions use 4 encryption layers: RSA2048, RSA1024, ChaCha, Salsa

**Step 2:** Double click BDFONIXDecryptor.exe and allow it to run by clicking yes on the UAC alert.

💡 User	Account C	Control		<b>×</b>
?		want to allow to this comp	the following progr uter?	am to make
	В	Program name: Verified publisher: File origin:	Bitdefender Tool <b>Bitdefender SRL</b> Network drive	
Sh	ow details		Yes	No
			Change when these r	otifications appear

Step 3: Select "I Agree" for the End User License Agreement





ADVANCED OPTIONS

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	
Bitdefender	×
Select This utility decrypts files encrypted by Fonix ransomware. The tool will attempt to find 'cpriv.key' on your system. The files cannot be decry This tool doesn't require internet access!	pted without it!
	ОК
START TOOL	DVANCED OPTIONS

**Note:** Tool informs that affected users, must have present on their PCs, at least 1 cpriv.key file, either in the target folder to decrypt, or anywhere else on disks.

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

We strongly recommend that you also select "Backup files" before starting the decryption process in case anything unwanted happens while decrypting. Then press "Start Tool".

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



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

Bitacremaci	Decryption Utility for Fonix ransomware.	<b>Z</b> —
	est ransomware protection 019 intercepts any kind of ransomware attack. BUY NOW	Bitdefende
can in r	progress	
	log below for more information	
Decrypt Fil	les	
		I
	full system	[OK]
Scanning f		[OK]
Scanning fi Decrypt [	full system 0] [C:\BOOTSECT.BAK.Email=[tt32styler32@cock.li]ID=[BD5D5592].XINOF]	
Scanning f Decrypt [ Decrypt [	full system 0] [C:\BOOTSECT.BAK.Email=[tt32styler32@cock.li]ID=[BD5D5592].XINOF] 1] [C:\LMKOD.Email=[tt32styler32@cock.li]ID=[BD5D5592].XINOF] [OK]	D5592].XINOF] [OK]
Scanning fi Decrypt [ Decrypt [ Decrypt [	full system 0] [C:\BOOTSECT.BAK.Email=[tt32styler32@cock.li]ID=[BD5D5592].XINOF] 1] [C:\LMKOD.Email=[tt32styler32@cock.li]ID=[BD5D5592].XINOF] [OK] 2] [C:\Program Files\7-Zip\7-zip.chm.Email=[tt32styler32@cock.li]ID=[BD5	D5592].XINOF] [OK] D5592].XINOF] [OK
Scanning fr Decrypt [ Decrypt [ Decrypt [ Decrypt [	full system 0] [C:\BOOTSECT.BAK.Email=[tt32styler32@cock.li]ID=[BD5D5592].XINOF] 1] [C:\LMKOD.Email=[tt32styler32@cock.li]ID=[BD5D5592].XINOF] [OK] 2] [C:\Program Files\7-Zip\7-zip.chm.Email=[tt32styler32@cock.li]ID=[BD5 3] [C:\Program Files\7-Zip\7-zip32.dll.Email=[tt32styler32@cock.li]ID=[BD5	D5592].XINOF] [OK] D5592].XINOF] [OK 2].XINOF] [OK]
Scanning fr Decrypt [ Decrypt [ Decrypt [ Decrypt [ Decrypt [	full system 0] [C:\BOOTSECT.BAK.Email=[tt32styler32@cock.li]ID=[BD5D5592].XINOF] 1] [C:\LMKOD.Email=[tt32styler32@cock.li]ID=[BD5D5592].XINOF] [OK] 2] [C:\Program Files\7-Zip\7-zip.chm.Email=[tt32styler32@cock.li]ID=[BD5 3] [C:\Program Files\7-Zip\7-zip32.dll.Email=[tt32styler32@cock.li]ID=[BD5D559 4] [C:\Program Files\7-Zip\7z.dll.Email=[tt32styler32@cock.li]ID=[BD5D559	D5592].XINOF] [OK] D5592].XINOF] [OK 2].XINOF] [OK] 92].XINOF] [OK]
Scanning fr Decrypt [ Decrypt [ Decrypt [ Decrypt [ Decrypt [	full system 0] [C:\BOOTSECT.BAK.Email=[tt32styler32@cock.li]ID=[BD5D5592].XINOF] 1] [C:\LMKOD.Email=[tt32styler32@cock.li]ID=[BD5D5592].XINOF] [OK] 2] [C:\Program Files\7-Zip\7-zip.chm.Email=[tt32styler32@cock.li]ID=[BD5 3] [C:\Program Files\7-Zip\7-zip32.dll.Email=[tt32styler32@cock.li]ID=[BD5D559 4] [C:\Program Files\7-Zip\7z.dll.Email=[tt32styler32@cock.li]ID=[BD5D559 5] [C:\Program Files\7-Zip\7z.exe.Email=[tt32styler32@cock.li]ID=[BD5D559 5] [C:\Program Files\7-Zip\7z.exe.Email=[tt32styler32@cock.li]ID=[BD5D559	D5592].XINOF] [OK] D5592].XINOF] [OK 22].XINOF] [OK] 92].XINOF] [OK] 92].XINOF] [OK]

If you encounter any issues, please contact us at <u>forensics@bitdefender.com.</u> If you checked the backup option, you will see both the encrypted and decrypted files. You can 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 bulk. We do not encourage you to do this, unless you doubled check your files can be opened safely and there is no trace of damage.

Ransomware in some cases encrypts files incorrectly so that decryption will not work properly, we recommend that you back up your files before using the decryption tool if you have not already checked the option "backup files " from decryption tool.

## Acknowledgement:

This product may include software developed by the OpenSSL Project, for use in the OpenSSL Toolkit (<u>http://www.openssl.org/</u>) and CryptoPP (<u>https://github.com/noloader/cryptopp</u>)