How to use the FunkSec ransomware decryptor

- 1. The first step is to download the decryptor binary. Avast provides a <u>64-bit decryptor</u>, as the ransomware is also 64-bit and can't run on 32-bit Windows. If you have no choice but to use 32-bit applications, you may download a 32-bit decryptor <u>here</u>.
- 2. Run the executable file, preferably as administrator. It starts as a wizard, leading you through the decryption process.
- 3. On the initial page, we have a link to the license information. Click the Next button when you are ready to start.

AVAST Decryption Tool for FunkSec v 1.0.0.750 (64-bit)	×
Wellcome We'll guide you through the process of decrypting your files. Click "Next" to begin.	
8 A	
License Information	
< <u>B</u> ack Next >	Cancel

4. On the next page, select the list of locations you want to be searched for and decrypted. By default, it has a list of all local drives, but you can pick a different list, such as a directory with important documents:

AVAST Decryption Tool for Fu	unkSec v 1.0.0.750 (64-bit)	×
	Select location(s) to decrypt fou can also drag and drop another location or file into this screen. Shortcut keys: DEL (delete), INS (insert), F2 (edit)	
	Add Local Drives Add Network Drives Add Eolder	
	< <u>B</u> ack <u>N</u> ext > Cancel	

5. On the final page, you can opt-in to back up your encrypted files. These backups may help if anything goes wrong during the decryption process. This choice is selected by default, which we recommend. After clicking Decrypt, the decryption process begins. Let the decryptor work and wait until it finishes decrypting all your files.

AVAST Decryption Tool for FunkSec v 1.0.0.750 (64-bit)	×
Backup encrypted files?	
We recommend that you backup encrypted files, so you can restart the proces later if something goes wrong.	s
Backup encrypted files	
E A	
E DT E	
Decrypt Cance	

For questions or comments about the Avast decryptor, email <u>decryptors@avast.com</u>.

IOCs

Ransomware sample

c233 a ec7917 cf34294 c19 dd60 ff79 a 6e0 fac5 ed6 f0 cb57 a f98013 c08201 a 7a1 c

Initial source code

7e223a685d5324491bcacf3127869f9f3ec5d5100c5e7cb5af45a227e6ab4603