GandCrab Ransomware decryption tool

Free Tools

3 min read

Bogdan BOTEZATU

October 25, 2018

Update June 2019: Our collaboration with the Romanian Police, Europol and other law enforcement agencies has yielded another new decryptor for all GandCrab ransomware versions released, except for v2 and v3. If you need to decrypt versions 1, 4, 5.0.1 through 5.2, then download and run our new tool linked below.

In February 2018, Bitdefender released the world's first decryption tool to help GandCrab ransomware victims get their data and digital lives back for free. But since then, victims of subsequent versions of GandCrab and its 'ransomware-as-a-service' affiliate approach have been reaching out to us for help.

The good news is that now you can have your data back without paying a cent to cyber-criminals. Bitdefender offers a free utility that automates the data decryption process.

Supported GandCrab Versions

The below table shows the versions of GandCrab this tool can decrypt and how to identify the version you have been inflicted with. You can recognize this ransomware and its version by the extension it appends to the encrypted files and/or from the first line of the ransom-note.

Version 1:	file extension is .GDCB.	Starts with —= GANDCRAB =—, ……. the extension: .GDCB
Version 2:	file extension is .GDCB.	Starts with —= GANDCRAB =—, ……. the extension: .GDCB
Version 3:	file extension is .CRAB.	Starts with —= GANDCRAB V3 =— …….. the extension: .CRAB

Version 4:	file extension is .KRAB.	Starts with —= GANDCRAB V4 =— …….. the extension: .KRAB
Version 5:	file extension is . ([A-Z]+).	Starts with —= GANDCRAB V5.0 =— ……. the extension: .UKCZA
Version 5.0.1:	file extension is . ([A-Z]+).	Starts with —= GANDCRAB V5.0.1 =— …. the extension: .YIAQDG
Version 5.0.2:	file extension is . ([A-Z]+).	Starts with—= GANDCRAB V5.0.2 =— …. the extension: .CQXGPMKNR
Version 5.0.3:	file extension is . ([A-Z]+).	Starts with—= GANDCRAB V5.0.3 =— …. the extension: .HHFEHIOL
Version 5.0.3:	file extension is . ([A-Z]+).	Starts with—= GANDCRAB V5.0.4 =— …. the extension: .BYACZCZI
Version 5.0.5:	file extension is . ([A-Z]+).	Starts with—= GANDCRAB V5.0.5 =— …. the extension: .KZZXVWMLI
Version 5.0.5:	file extension is . ([A-Z]+).	Starts with—= GANDCRAB V5.1 =— …. the extension: .IJDHRQJD

Decryption Tool Requirements

- **Active Internet connection.** This tool REQUIRES an active Internet connection as our servers will attempt to reply to the submitted ID with a possibly valid RSA-2048 private key. Only if this step succeeds will the decryption process continue.
- **The ransom-note.** For this recovery solution to work, you must have at least (1) copy of the ransom-note on your PC. The ransom-note is needed to recover the decryption key, as it allows us to compute the unique decryption key for your files. Please make sure that you do not run a clean-up utility which detects and removes the ransom-note prior to execution of this tool.

How to Use the Tool

Step 1: Download our decryption tool and save it somewhere on your computer. Please note that this tool requires an active internet connection. Without it, the decryption process won't continue.

Download the GandCrab decryptor

This tool REQUIRES an active internet connection as our servers will attempt to reply the submitted ID with a possibly valid RSA-2048 private key. If this step succeeds the decryption process will continue.

Step 2: Run the utility. It should be saved on your computer as BDGandCrabDecryptor.exe.

Step 3: Agree to the terms and conditions.

Step 4: Select “Scan Entire System” if you want to search for all encrypted files or just add the path to your encrypted files. We strongly recommend that you also select **“Backup files”** before starting the decryption process. Then press “Scan”.

Regardless of whether you check the “Backup files” option or not, **the decryption tool initially attempts to decrypt (5) files in the provided path and will NOT continue if decryption is unsuccessful**. This extra safety mechanism ensures that the decryption tool has yielded valid files. This approach will however, impact potential tests ran on 1 or 2 files, or rypting files with different extensions.

Step 5: At this point, your files should be decrypted. If you selected the backup option, you will see both the encrypted and the decrypted files. We recommend that you now validate that your files may be safely opened and there is no trace of damage.

Once you have validated your files, you can remove the encrypted files in bulk by searching for files matching the GandCrab extension.

If you encounter any issues, please contact us at via the e-mail address provided in the removal tool.

Acknowledgement

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)

TAGS

free tools

AUTHOR

Bogdan BOTEZATU

Information security professional. Living my second childhood at @Bitdefender as director of threat research.