

## GANDCRAB RANSOMWARE DECRYPTION TOOL

### Technical description:

This tool recovers the encrypted files, affected by GandCrab ransomware (V1,V4,V5). You can recognize this ransomware and its version, by the extension it appends to the encrypted files and/or ransom-note:

Version	Extension	Ransom-note Info
1	.GDCB	---= GANDCRAB =---, ..... the extension: .GDCB
2	.GDCB	---= GANDCRAB =---, ..... the extension: .GDCB
3	.CRAB	---= GANDCRAB V3 =--- ..... the extension: .CRAB
4	.KRAB	---= GANDCRAB V4 =--- ..... the extension: .KRAB
5	.([A-Z]+)	---= GANDCRAB V5.0 =--- ..... the extension: .UKCZA ---= GANDCRAB V5.0.2 =--- .... the extension: .YIAQDG ---= GANDCRAB V5.0.2 =--- .... the extension: .CQXGPMKNR ---= GANDCRAB V5.0.2 =--- .... the extension: .HHFEHIOL

In order for this recovery solution to work, you are required at least 1 available ransom-note on your PC. The ransom-note is required to recover the decryption key. Please make sure that you do not run a clean-up utility which detects and removes these ransom-notes prior to execution of this tool. The information inside the ransom-notes, taken as input for the key-recovery procedure, may look in one of the two ways, shown below. Judging by this information, GandCrab ransomware had a significant shift since January 2018, which relates to encryption mechanism.

### GandCrab V1,V2,V3:

---= GANDCRAB =---

Attention!

All your files documents, photos, databases and other important files are encrypted and have the extension: .GDCB  
 The only method of recovering files is to purchase a private key. It is on our server and only we can recover your files.  
 The server with your key is in a closed network TOR. You can get there by the following ways:

1. Download Tor browser - <https://www.torproject.org/>
2. Install Tor browser
3. Open Tor Browser
4. Open link in tor browser: <http://gdcbgvhvjqy7jclk.onion/cc9e5e748005>
5. Follow the instructions on this page

If Tor/Tor browser is locked in your country or you can not install it, open one of the following links in your regular browser:

1. <http://gdcbgvhvjqy7jclk.onion.top/>
2. <http://gdcbgvhvjqy7jclk.onion.casa/>
3. <http://gdcbgvhvjqy7jclk.onion.guide/>
4. <http://gdcbgvhvjqy7jclk.onion.rip/>
5. <http://gdcbgvhvjqy7jclk.onion.plus/>

On our page you will see instructions on payment and get the opportunity to decrypt 1 file for free.

**DANGEROUS!**

Do not try to modify files or use your own private key - this will result in the loss of your data forever!

## GandCrab V4,V5

```

---=  GANDCRAB V5.0.2  =---
Attention!

All your files, documents, photos, databases and other important files are encrypted and have the extension: .YIADGG
The only method of recovering files is to purchase an unique private key. Only we can give you this key and only we can recover your files.
The server with your key is in a closed network TOR. You can get there by the following ways:

-----
| 0. Download Tor browser - https://www.torproject.org/
| 1. Install Tor browser
| 2. Open Tor Browser
| 3. Open link in TOR browser: https://gandcrabmfe6mef.onion/d870d3cc22be493d
| 4. Follow the instructions on this page
-----

On our page you will see instructions on payment and get the opportunity to decrypt 1 file for free.

ATTENTION!

IN ORDER TO PREVENT DATA DAMAGE:

* DO NOT MODIFY ENCRYPTED FILES
* DO NOT CHANGE DATA BELOW

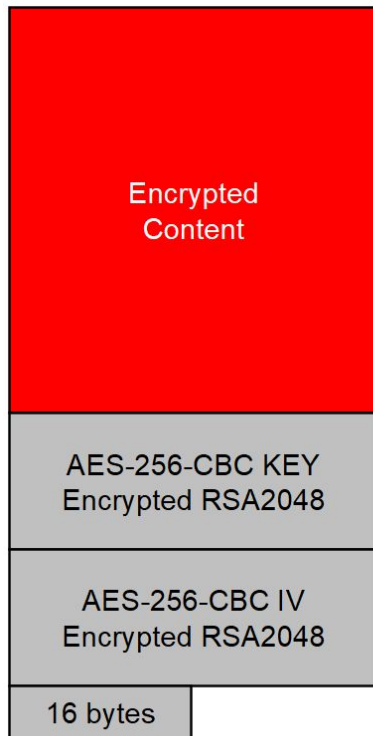
---BEGIN GANDCRAB KEY---
1A0AAHMZarKrc1he4ud38T58996ENDd72e+1w/Ugux3860zR2M1LxeAaCkV/3pj1k+KvWkR20p9xWC1q4pp+NHFPQ+H4d28/7Iuznt0eWu5Coux82ifds1aa4cSTd5e0fcklqk1/ADT8226ZKx153jwVjVnrMocV/ptrSVW/ux1AK6E6M1r+3j0
Xz+RnRCG82daqsK1rgF10UglY0wSE7VRHTI5RkKScayleKuDFPKq53JcAsdFQKkhQ/2j+JrNN2gHZTQyqEVNMRnt2MT96dJUNQhA9bbt51Ct+Iu0TncgFgW/Ofslg1Tvj1TDOY63mlSabIbbrYBR5Q3eDcLgEU0u8874nRRg7r1YA3I37/F4V61AAWnLx
M5WuZTfEjPjbnmz72aL2LkXv8K7C2E1dASN6K1Xkz2AeHd1KkFuvu2CAUURMLB3UOTD6M90j27hXQq8FtY85dq+NBBCA1V5+95qye4dL/80Ij+rEtUvImn08RcywM8lEQuQNCNz21KURkV1K5dt/L5nCFtE06XJNzr7kVGDCT7deoNWKdcl18E
W7AKXhMwMa7EUF7L3J4cFwP+HaaVhDaI3cKMS8+9/7Pp+g8Mqy2o1R3Dw+SBz2URsh5Fc1FBRRB3FKK070ZhdIKK7rDMqndDg+IAR)6p112c7LCTtVhM4E4v55qYI6c18Jn1T0dL46E7Jb9gKec106E1JhV9T2VxxK5GyV7pW21b38Q6N
ty80G6ChT5Z4VERJ7r7qda6JgBaBspHWH43M4q6V0c1sMM83w3Rvmpj9gRcdkTJkCk030dubhQW/STQPe1dQ1r2kTeYk3Qp8R2aCkbeEVBjy61U919wBa+1h4t61D11*31dc4dmm4dM41Dwca7nD6e30E10Ufpa59cF215f
YFGcuFSeoF8tYCW3w0dYr1UH1xMgqKCRJWSzJ8336Qko26R998KeTDXVH5GTF12ziQU1+dePrdDMU0Bna+0/RvEgM3+584c86tr9HATMqVdWJQJoSOD1cXMBYIK44pdpkXnIbpx+gEc4Bj98pXp7FsekhUbnLrFoQcm17KAt1j3t4PHTF6/EcuH
naWU2RTJ2078Fy9sh02071ascXBFZHQV4M3WcRQ3k15Aov6VEpzk3WNAyCrsUzrE16tBDYLD21ek2Pfga/jEobkS91yCrfw3D85/9kLo33jz273guImE9k+K4G8JWvRxaAmV30UTZj6o2z/KK41S668y8w10qa1B6K4F010vPpOQqyU14
Sx18qc2I+AU010oRDh31B112qzr1TS0v+JKH+VwQNf0y4CFDPaV5j3oM01jP2HA0LB8dmCKedWgT2qba/RQDnlp/SEZuChCtFDy61gZ/f7zfc7Qq7br4ljrksavZG//7heHash4tj9NG/Fy5on3v15r/LeEwLR3kU9v9V32H6wMcy7Ahs9e
CS1e1j3X00F4annJdC8dM2C0cevFNZr1uLkLWbIacVrth8J1hFSPgM1T3f98c36gFsqD46rpdgP38qZNa/1bwVcRnlpGXAX1Y5fCk22/De6bYXUcWbRwM1jha7HQJ5sd2MOV7xy1hns2563cTdq7gqXmFRJy1Vr110E8XG2+o8B00VUJJa1sUx316b1c
Rw1VcVXFfY0T0eW10y120k377428U0Y75MXXAU/LJ3w61/KAln50dNnm4pCgt23p/bnLuUu+ahzYuQ3jgAy7p3h000/XacRrEyg58214bIXdbrnUIIkUhmeyubrA3F61gE7kAD0P2ERP45ioh9eK2L2mL5433Bmdp9WndJX4dG5hv3IHGL++20CzqFVf
aFJAP9V9eJp1gi6z82dknvtDBS1PnrhSv864972RQ2d+4fLVxv+mz2yM2C2gxn0nJrFcvdgd+ynLJ2gA+FLINtBHq4EE796Uw2Om8pFIWkQo4uEfhEhsEyyJ6e9eINhK25V0yAE2z+Ya7pCh71aut5x8PfwV7R5e0QcQ1eIauEBqkGtbRvc31e
F1MFKJ1XcGMqG54F79e81rTE9YgrnsD9vMlB8SGt4LcuuJX8UB8Qm6v5Fwz241YadV620DhpxELeX1LeccS3KLU8H8A4wDKRivH/F9smF1RMV9W8aH/504E1QV=
---END GANDCRAB KEY---

---BEGIN PC DATA---
wFD61udumBmpL8IR44956xPFA10T3t3j3jOpv1k1Yov0uWnX4WY21dy2ZaTvpRrnYg7h5W1bf2TH6Hx50B3DmdM7/16akGoDbV1pJW8+/FCV/6mH6od2A5LrUj6FkX2VxP2K6iyOh5K53Av1Arz240KX8LxNw8kYXqy2GwqcdYc1YDKS0xtQpK
Y4g29QAT1KZALVAP68uUfcoN5Y2P2MFU0oM0YFgIodL6GTzTmtIoRZ+P6Q/UPrM1s1zhTbPjYIAG3g8165nV40/CBUxRQ7KDjYrXovSnnFg/ykfgtJN1wqfCngbr8+Bit7F6K1/B40Lw/2U2QutLg1YblrBnLrqrHFEdb095cE4o64b6a1Y82yGo
yp2Q2iuJrsTRoq1PQJ1c0JoJrWnoBBPjNkV+CO5cALqfj2Epgf1rLw3cxAhKyQ7wZ1fpDRFF3vbLM+all2w203R0R1CKAtm1jXgAm9imUkfsz70UxnnL1s12w73IMV7/pezyfAcceMBjP9JmInXQ3j3KZKkEdKkiGy1M5e5G8s40cb/Rd8Peak
9V+butLonzJ/9bHYh8c2e6xerbtcc/+YbnzW5+J0X5e5PtQo9Fxn0LLD2rxghGmLLQ0c3Qtdfj30GFT1rWEn7J7T+zb
---END PC DATA---

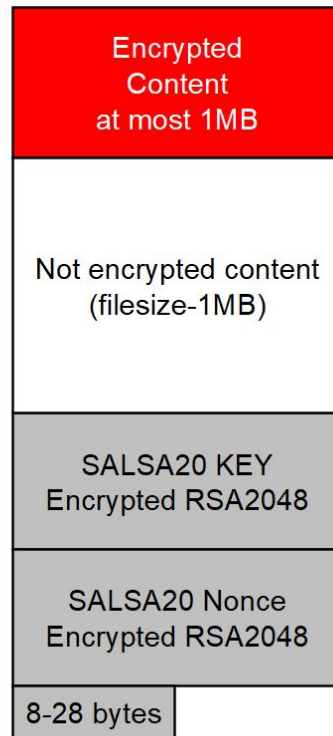
```

The shift of the ransomware was about using a different encryption type and, and if versions 1,2,3 of the ransomware used AES-256-CBC, versions 4 and 5 use Salsa20.

The ransomware kept constant the encryption flow, but considered the damages they have done to files exceeding 4GB in their first versions, and now they only encrypt at most 1MB.



GandCrab V1,V2,V3



GandCrab v4,v5

## Steps for decryption:

**Step 1:** Download the decryption tool from

[http://download.bitdefender.com/am/malware\\_removal/BDGandCrabDecryptor.exe](http://download.bitdefender.com/am/malware_removal/BDGandCrabDecryptor.exe)

and save it somewhere on your computer

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

**Step 2:** Double-click the file (previously saved as BDGandCrabDecryptor.exe) and allow it to run by clicking Yes in the UAC prompt.

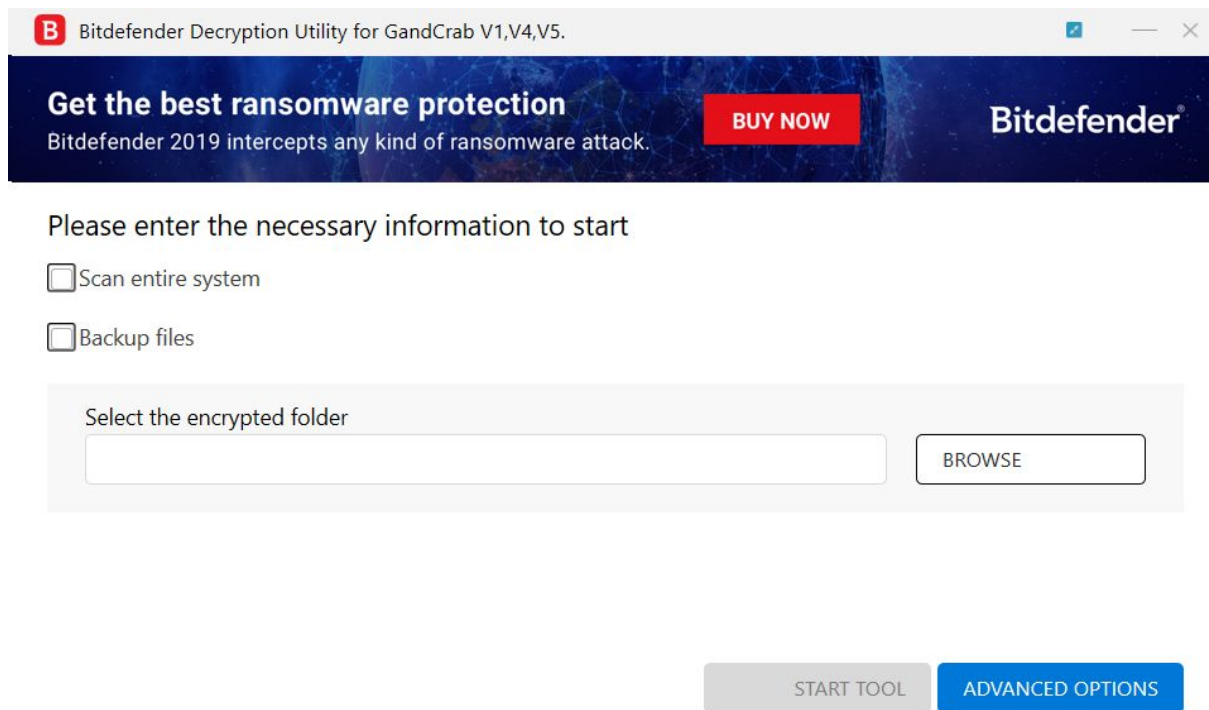


**Step 3:** Select "I Agree" for the End User License Agreement



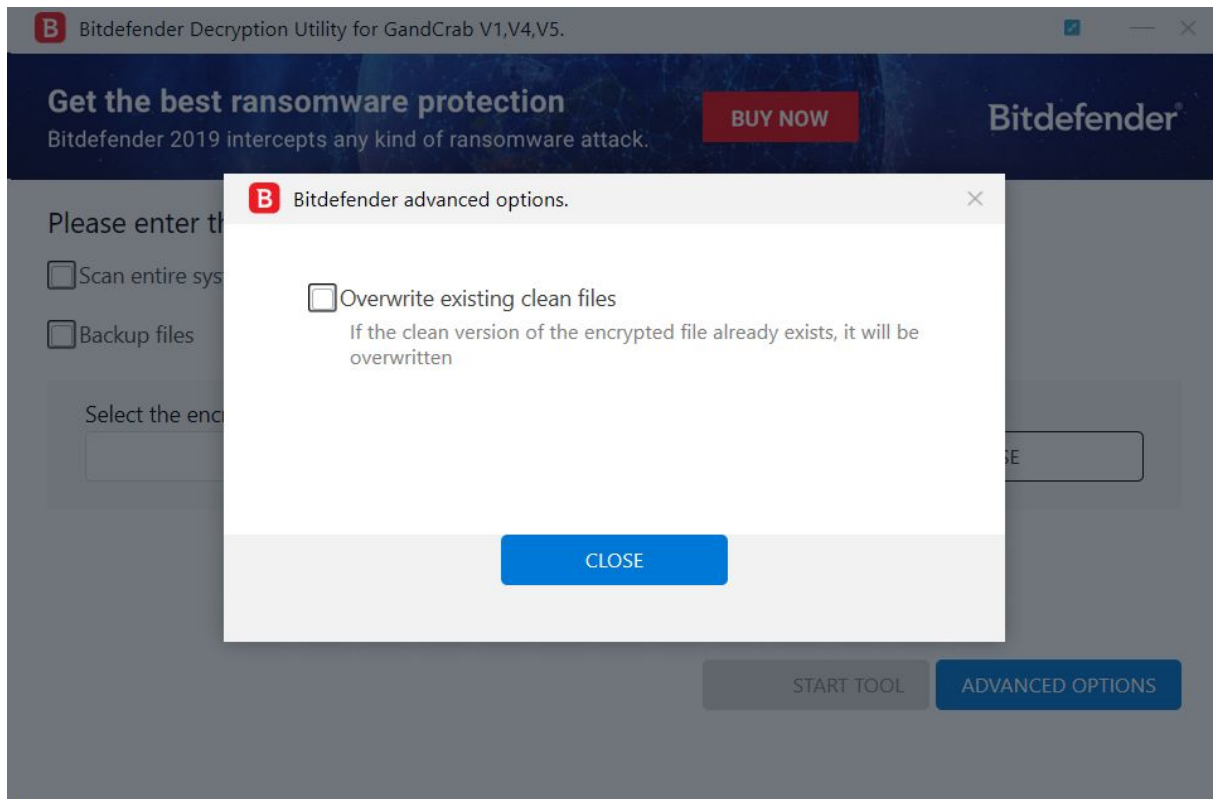
**Step 4:** Select “Scan Entire System” if you want to search for all encrypted files or just add the path to your encrypted files.

We strongly recommend that you also select “Backup files” before starting the decryption process. Then press “Scan”.



The screenshot shows the Bitdefender Decryption Utility for GandCrab V1,V4,V5. The window title is "Bitdefender Decryption Utility for GandCrab V1,V4,V5". The interface features a dark blue header with the text "Get the best ransomware protection" and "Bitdefender 2019 intercepts any kind of ransomware attack." A red "BUY NOW" button is visible. Below the header, there is a section titled "Please enter the necessary information to start" with two checkboxes: "Scan entire system" and "Backup files". A text input field labeled "Select the encrypted folder" is followed by a "BROWSE" button. At the bottom, there are two buttons: "START TOOL" and "ADVANCED OPTIONS".

Regardless of whether you check the “Backup files” option or not, the decryption tool attempts to decrypt **5 files** in the provided path and will NOT continue if the test is not successfully passed. The chances that something goes wrong are actually low, however we make these supplementary checks to make sure that nothing goes wrong nor on your, nor our side. This approach may not suits some testers, which might want to decrypt 1-2 files at most, or not conforming file extensions. Users may also check the “Overwrite existing clean files” option under “Advanced options” so the tool will overwrite possible present clean files with their decrypted equivalent.



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

If you encounter any issues, please contact us at [forensics@bitdefender.com](mailto:forensics@bitdefender.com).

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.

### Silent execution (via cmdline)

The tool also provides the possibility of running silently, via a command line. If you need to automate the deployment of the tool inside a large network, you might want to use this feature.

- **-help** - will provide information on how to run the tool silently (this information will be written in the log file, not on console)
- **start** - this argument allows the tool to run silently (no GUI)
- **-path** - this argument specifies the path to scan
- **o0:1** - will enable **Scan entire system** option (ignoring **-path** argument)
- **o1:1** - will enable **Backup files** option
- **o2:1** - will enable **Overwrite existing files** option

**Examples:**

**BDGandCrabDecryptor.exe start -path:C:\** -> the tool will start with no GUI and scan C:\

**BDGandCrabDecryptor.exe start o0:1** -> the tool will start with no GUI and scan entire system

**BDGandCrabDecryptor.exe start o0:1 o1:1 o2:1** -> the tool will scan the entire system, backup the encrypted files and overwrite present clean files

**Acknowledgement:**

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