

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: .YIAGQG
The only method of decryption is to purchase a 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:

-----
1 0. Download Tor browser - https://www.torproject.org/
1 1. Install Tor browser
1 2. Open Tor Browser
1 3. Open link in TOR browser: https://gandcrabmfe6mnef.onion/d870d3cc22be493d
1 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

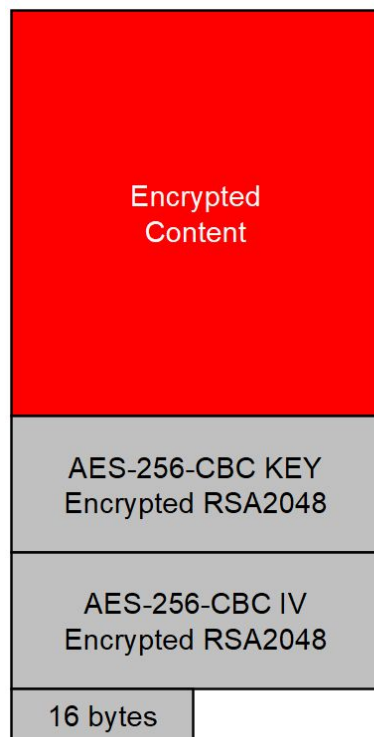
---BEGIN GANDCRAB KEY---
1AQAARHMZarKrihe4u38T58996ENDd7ze+zrN1/wUgux38e0zsr2MNLxeAacKxv/3pjr1k+KvnmK82Qp9xwC12q4ppV+NzHPQ+H4d28/7Iuz2nt0eWu5Coux82Ifds1aa4icSTd5z0fcklqk1/ADT8226ZKx15kjwVvnrMacV/ptrSvM/ux1AK6d6M1r+3j0
Xz+RnHC82daqeK1rgF10UglY0wSE7VRHTI5RdK5cayleKuDFPKq53JcAsdFQNhQ/2j+JrIN2gH2TWQyEVNRRnt2MT96dJUNQhA9bbt51Ct+Iu0TncgPdWZ/Ofs1glTvj1TD0Y63mlSabIbttYBR5Qj+DzLgEU0u8874nRRg7r1YA3T37/F4V61AAWnLx
M5WuZTfipE9jblmz72aL2LkXrvbTMC7jC2E1dASH6K1XkzdzAeHd1KkFuvu2CauURMLB3J0VOTD8Mw0j27hXQq8Fiy85dq+RNBCKA1V5+95qye4dL/80Ij+RtOvLmno8gRcywn8lEQuQWcNz2LKRRkv1X5dt/L5nCFteD6XJDNz7KVGDCY7de0NRWdcl18E
W7AKXtNmWa7EUF1cJ14cFwP+HsaVhSa13CRX58+9/V7p+gRmCgzc01R3DWc5Bc2U8sh5Pc1FBRHR3FkkQ70y2HdIKF7zRMqntD5+1ANj6p112c7LcTtVhMEH4v5SgITMcF18Jn1TQdLAc6EJbGgITMc10661JhV5T2vxxK5GyVapw21bb3RQ4Nq
ty80G6ChT5Z4VERJ7ztgAdw6JgBaBapHWH632M4q64V0c1+Mw68w3dRvnyfEp8pCdd6JALcRz03d0uhQW/STQPe1dQ11rhtYkSh3Qm5i2aCzbeFVYgYMaT091gW8a+1h4T61D11*731dr6dmdKdMa1DwcenJdG630P10UPgwa59p82e155
XPGouFSoe0FstVCW3w0Ayt+UHLvXMGpKCRJWSzJ8o36Qko26R998Ke7DXVGH5GTf12ziQU1+dsPrdDMWU8na+0/RvEpM3+5B4cB6tnr9HATAJgVdWJQJo50D1cXMBVIK84btpndkXnIbpx+gEc4Bj08pXpvt7EehkU8nTLrFoQcm17KAtz1374PHTF6/EcuH
uuWU2RTJEO78Py9shhA2Q71acXBF2HQvM3HwRQ3k15fAov6VEpzk3WllyCraUzrE16tBDYLD21e1k1p2IFga/JEobK91yCrfw3DHS/9kLo33jzr273guImE5kq+K4G8JWvRxaAmV30UTZj6o22a/K5415688yeeW10eqalB6K6F001DoVP0QqyU01+
SxS18gcJ2+AUb01o0RDhB112q2r1TS0v+JKH+VwQnf0y4CFDPAV9jz0m01jP2HA0LB8dmCKedWgTygob2Qba/RQDtnOh/SEZuCHCzF1D6ylgf/77zfc7QqJbr4ljrkasvZG//7TheHash4tj9NG/Ffys0nJzV15r/LeSewLR3kUw9Vsv32H6wMcy7Ans9e
C5ie1j3XXOPX4anuJdc8dW2C0cevFwZRLuLkLWBIacVrth6J1hF5GMI73f9Bc36g3Sqd46rpdgF38qy2Ne/1bwzVcrnlpGXAX1Y5IFcX22/De6bYXuCwBRWmljha7HQ75sdZMOV7xyThnS2563cTdg7q6XmSFRJy1VrV11OE8XG2+o8B00YVUJAlaUx3I6b1c
8w1VcVXFfY0T6W10y1j20k37128UY0u75MXAU/LJ3w61/KALnS0dNnm4pCgt23p/bnLuUU+JahzYuQ3gYg7p3h000/XacRr6yG58214bIXdbrnU1IkTuRmyeubrA3F61gE7kAD0P2ERF42ioh9cK2L2mLs433Bmddp9WndJXdAG5hV3IHGLc++20CzqFVZ
uFZAP6Y9j5pJg1v62n84kmvtDBS1PnR8V864072RQed+4FLVxv+mz2yH2C2gxn0nJzFcvdgd+ynLJ2gA+FLINXBRG4EE79G0w2Om8pFIWkoQ+4uEfhEhsEyyG9e9eINhK25VQyAE2+Ya7p8Ch71aut5xBPwKyFVJr5eOQc+QleIauEBqKgbRvt31+e
FIMFKJ1XcQM2G54KF19e81cTE59YqgnsD5vmlG8SGC41CuuJX8UB6QM6Gv5FWz241YadV62009hweFL6k+1ecn53KLU8H8A4wDK8r1v8/F9smF1RMV9W8a1W/S04E1QV=
---END GANDCRAB KEY---

---BEGIN PC DATA---
wFND61udumBkmpL8IR4U56xPFA10T3t3j3jOpv1k1YovOuWnX4WY21dy2ZaTvpRrnYc7h5W1bf2TB6Hxx5oB3JdmdM7/16akGoDBv1JpJW8+/FCV/6mH6od2A5Lruj6FkX2VvxP2K6iyOhSK53Av1Arz240KX8LoXW8kYXQyb2GWqcDcYc1YDKS0xtQpK
Y4g290AT1KZALVAP8oUf6nS5j22MFU0oMYpJocL64TGzTmtIoRXZ+P6Q/UPrM1slzhTbpjYIAG3g165nV40/CBUxKQ7KDYrXovSnnFXg/ykfgtJNiwqfCngbr85+Bit7F6KJ/B40Lw/2U2QutLgt1Yb1rBnLtgRBFEdob95CE4o46b6a1Y8ZyGo
yp2Q21uJr8TRoqJ1PQJ1oJfTcWfocMBBPJnKw+C05cALqfj2Epg61rLw3oxAhKyQ7wZ1fpDRFF3vblM+all2w203R0R1CKATmljXgAX9imUzfkS27UQxnnL1a1e2w31M7V/pezfYfAsceMBjP3JN1nXQ3j3CKZKEudtKvlgBY1Me5G8H40cB/KRd8Peak
9V+butL0nzJ/9bHYH8c6u8eRbttC/+YbnzW5+J0X8ePtQ9Fxb01LD2rxghGmLLQ03Qtdfj3j50GFT1RwEn7JfT+zb
---END PC DATA---

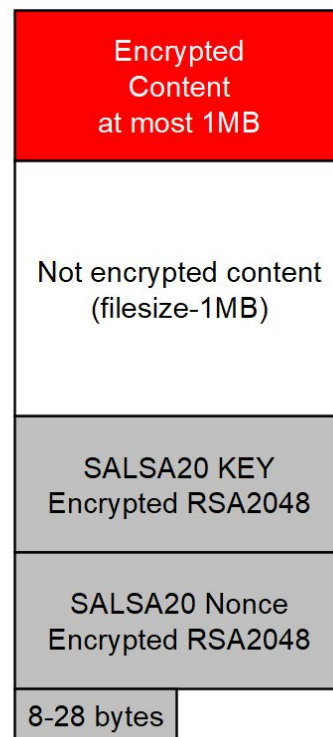
```

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

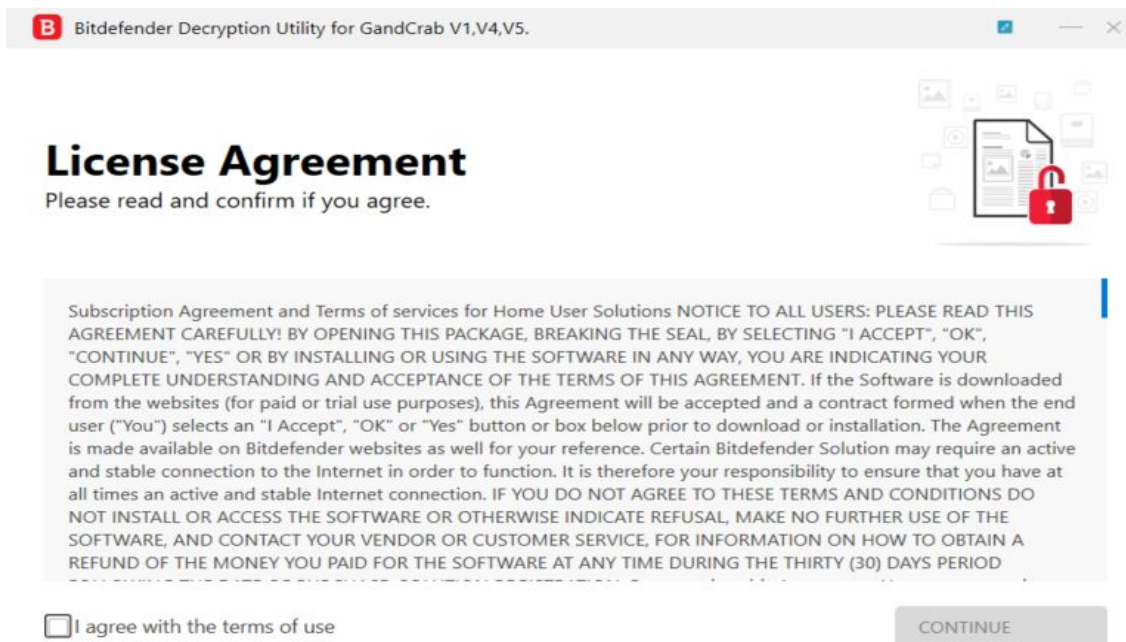
and save it somewhere on your computer

*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.

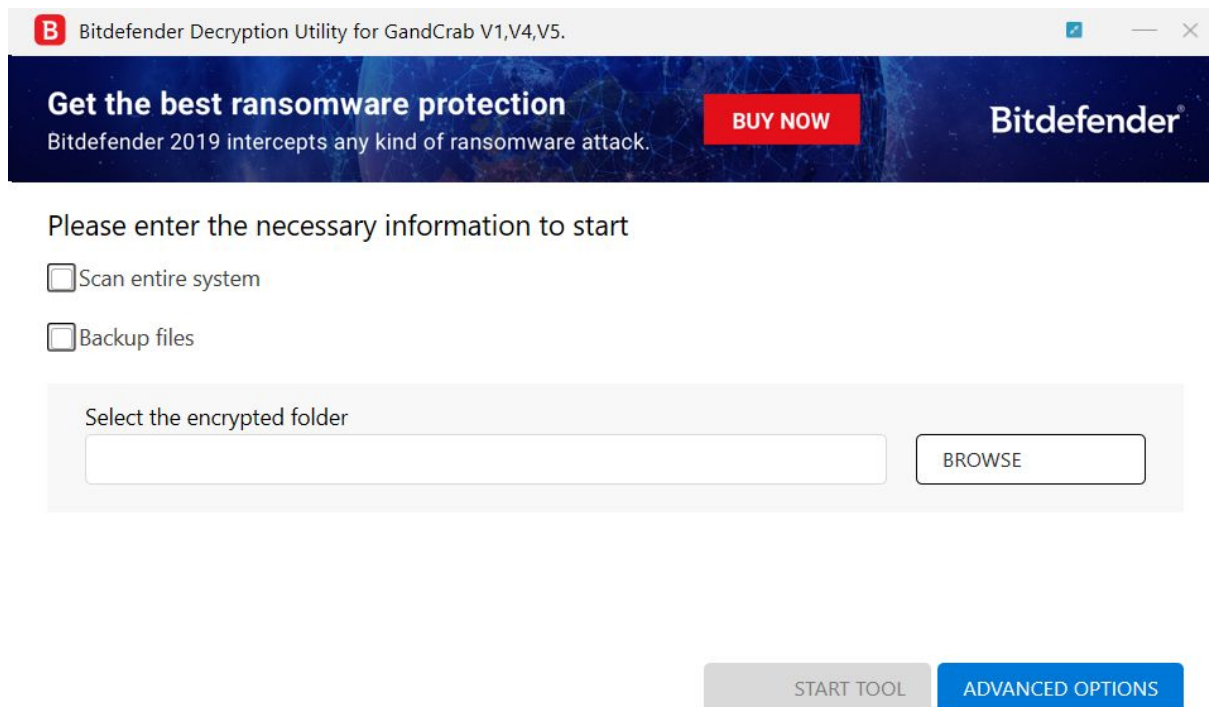


Step 3: Select "I Agree" for the End User License Agreement



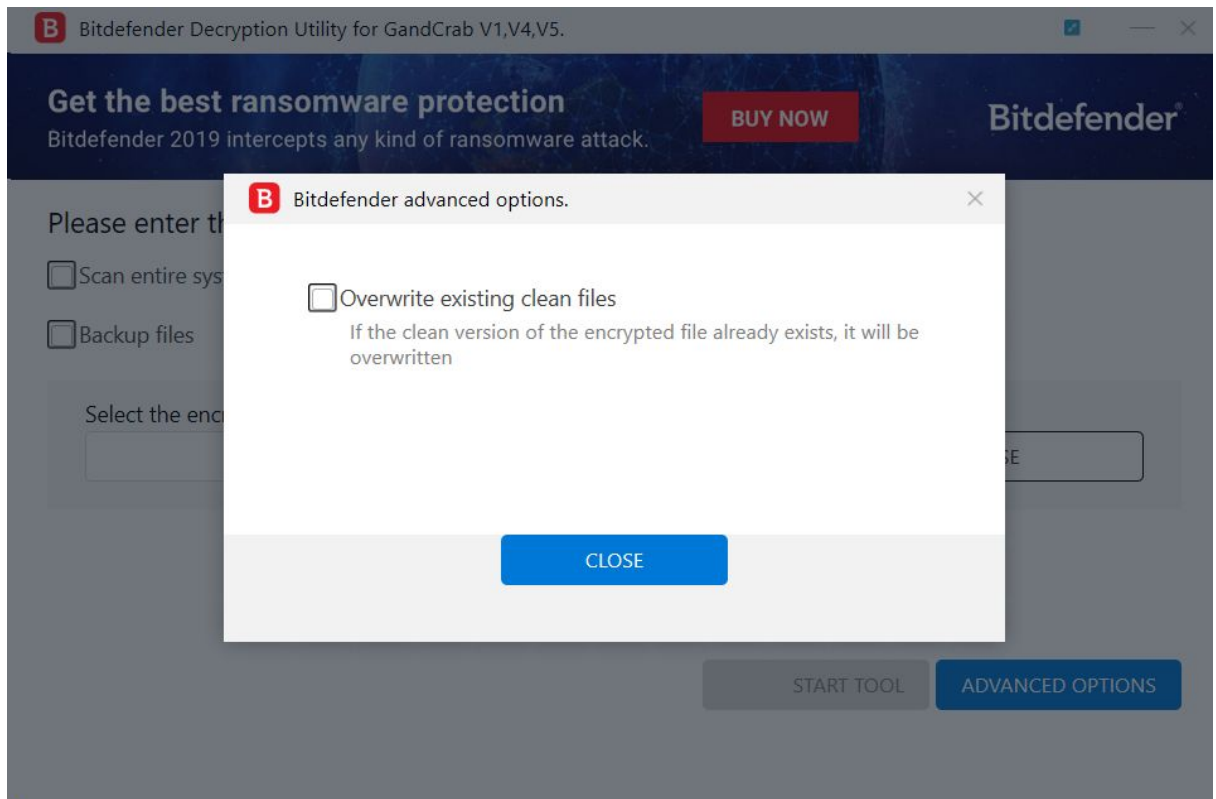
Step 4: Select “Scan Entire System” if you want to search for all encrypted files or just add the path to your encrypted files.

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 has a dark blue header with the text "Get the best ransomware protection" and "Bitdefender 2019 intercepts any kind of ransomware attack." There is a red "BUY NOW" button and the Bitdefender logo. Below the header, the text "Please enter the necessary information to start" is displayed. There are two checkboxes: "Scan entire system" and "Backup files". Below these is a section titled "Select the encrypted folder" with a text input field and 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.

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/>)