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:

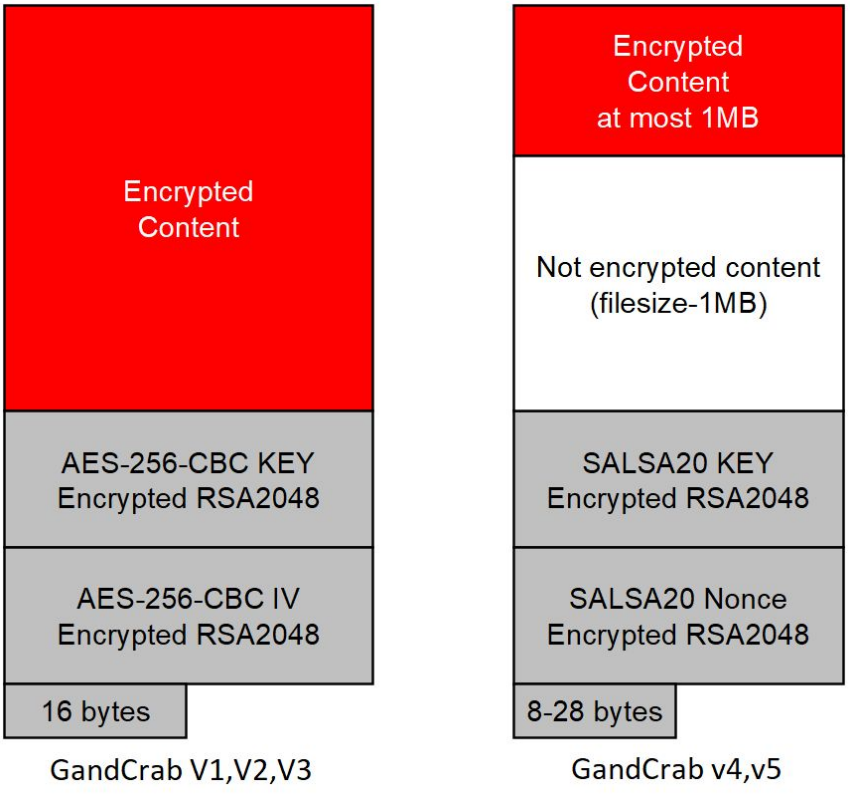
```
---= GANDCRAB =---

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://gdcbghvjyqy7jclk.onion/ce[redacted]
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://gdcbghvjyqy7jclk.onion.top/[redacted]
2. http://gdcbghvjyqy7jclk.onion.casa/[redacted]
3. http://gdcbghvjyqy7jclk.onion.guide/[redacted]
4. http://gdcbghvjyqy7jclk.onion.rip/[redacted]
5. http://gdcbghvjyqy7jclk.onion.plus/[redacted]

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: .YIAQDG
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:   http://gandcrabmfe6mnef.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---
lAQAAHMZarKrihe4uD38T58996ENDu7Ze+rNl/wUGux386o0zsRZM0lxeAsCKxv/3pjrlk+kVnwKB2Qp9xWCIZq4ppY+NfHPQ+H4d28/7Iuz2ntOeWu9Coux8ZIfdsIaa4icSTd5z0fcklqkl/ADT8226ZKxi5xjwrJVwrMxcV/ptrSvM/ux1AK6d6Mir+JjO
Xz+RnHCG82daqsKirgFl0UglY0oW5E7VRHTI9KdkScaylekuDPPKq53JcAsdFQNkhQ/2j+JrNN2gHZTWQydEVMNRnt2MT96DjUNQhA9bbt5lCt+Iu0TNcgFdWX/Ofslg1TwjiTDOY63mlSabIbbtYHRSQjsDzLgEUoNu8874nRRq7rlYA3T37/P4V6lAAWnlx
M5WuZFIp6PjbNmz7ZaL2LkXrvBkTMC7jC2ElAdASN6KlXzkdzANeHdlKkFuvu2CAuUKMiB3JVOTD8MW0j27hXQqsPIy85dq+NNBCkAlV5+95qye4dL/80IjrRtUvLnm08gRcywnBlhEquQNcNxZlKDRkvlxSdt/LSnCFteD8XJDNzr7kVGDCY7deoNWKdtl18I
M7AkXtNmwWa7EUFLt3T4tFeWp+NzaVhdSaI8CKx58+9/VYp+gRmOgzOlR3DWc5Ht2UKsh5PcIFBGRHHJFkkQTUyZNdlKf7rDMqnrDG+lANj6plI2cY7LCfTtvMmEN4E4v5SqgYMcF18JnITQdDiA6fEJbGgTXecl086TJhV8TZvxxKSCgVUrpw2ibb3RQ6Nq
zyHGU6ChTSZ+VFRJfs7gAdw8JgExBaapHWN63zM4q6aV80cls4M6f8xw3bRvnyEq9RpCdd6JAicKz0JdGuhOW4/STQtPe0ldQlirkhTtYkSn3QhGiK2aCzkbefBVgyMaIU91gw+Ba+Ih4TdlDli73Idr6ddmvMdzMLalUwcaJnUGe3OP1UUPgwat9cpK2s15f
XFGcuFSoeOF8tYCW3wDAytiUHlvMgqXCRJWSzJSo3€Qko26R998Ke7DXVGN5GTFl2ziQUI+dzPrdDMWUBmA+O/RyEpM3+5B4cB6tnr9HATAXgYDwLQJo5ODIcXMBVIKB4phpndxXnIbxp+gEc4RJG8pXprTFsehkU8nTLrEoQCmi7KAtzljzT4PHTF6/EcuW
uaWU2RTjE07t8Py9xhAQ27lscxXBfZHQkVdM3NwcRQ3ki5fAov6VEEpzk3WNayCrsUzrEI6tBDYLdZle1kpZIFqa/jEobkS9lyCrfw3DH5/9kLo33jr273guImE9kp+K4G8JWvRxaAmV30UTZj6oZZs/KK4lS6G8yssWi0sqalBA6K4P0OlDoVPzQQqyQl+
SxSI8qCc2I+AUb0loORDhjBIi2qZrlTSOv+JkH+VwQNfoy4CFDPaAV9jz0m0ljPZHAOLB8dmCKsdWqTygobZQba/RQDtnOh/SEZuCHCtFIDéylgf/f7zfCz7QqJbr4NjrxasvZG//7heHush4tj5NG/PfysOnJsVi5r/LeSEwlR3kUw9VsV32H6wMcy7Ahz9e
C5iEIj3XXOFXa4nuJdC3dNI2cOcewFNZRluKLwBiacVrht8JlhFSgMIT3f9Bc36gfSqD46rpdgP38qyZNa/IbwrVCrnLpGXAXiYSIFcX22/Ue6bYXuCwbRWmljhA7KQJ5sdZMOVTxyIhnS2563cTdq7q6XmSFRJjylVtVllOE8XG2+o8B0OYVUjAlsUx3I6blc
KwlVcVXFPyOTO6Wloyij20kJ37iZ8UYJu75MXAU/LJ3w6l/KAinS0dNNm4pCgtZ3p/bnLuUU+jahzYuQ3jqAy7p3hOOO/XacRr6yG58214bIXdbrnUIIkIuHmyeubrA3F6igE7kAD0P2ERP4zioh9tK2L2mLz433Bmddp9WndJXdAG5hv3IHGLt++2OCzqFVI
uFJAP8Vy9sJplgiv6Zn8ZdknvtDB5iPnRhSV864G72RQrd+t4flVxv+mrZyM2C2gxn0nJrFcvdqd+ynLJ2gA+FlNIxBHg4EE79GUwZOm8pFIWkcQo4uEFhEhsEygJe5sINKhk25VQyAE2t+YsJp8Ch7laut5xBPrWxyPVJR5eOQczQleIauEBqkGrbRvt3i+e
fIMFKJlXCgM2oG54KPi9e81tTESQYqqnzD9ymNdBSGt4LcuuJX8U8€QMzGySfWzZ4iYadV620D9bwgELqX+lecnS3KLUBHsA4wDkRjvH/F9smFlKMVWHqiN/SO4EiQY=
---END GANDCRAB KEY---

---BEGIN PC DATA---
wfKD6iudumBkmpL8IRr4U56xPFaIOT3tjxjOpvlxlYovOuWNx4WYZldyZZaTvpRrnYc7h5Wlbf2TH6Hxx5oBJDzmdMV7/L6akGoDBviJpJW8+/FCv/6mH6odZA5Lruj6PxX2VvxPZKGivOhSkS3AvIArrZ4OKCX8LnXbW8kYXQybZGWqcDzYclYDKSOxtQpK
Y4g29OATlK4ZAlVvAP8uUfcNSJy2P2MPUOoMOYPgIodLG6TGZxTmtIoRXZ+P6Q/UPrMlslzhTbpjYlAG3g8165nVd0/CBUxKQ7KDJYrtXOvSmnFXg/ykfgtJNiwqfCnqbr85+Bit7F6kU/B4OLw/2U2Qut1GtlYblrRBnLtqRHfEdob9ScE4oG4b6alY8ZyGo
yp2Q2iuJRzTRoqGlPQJIcJoJFtwNooBBPJnKw+CO5cALqfj2Epg6lrLw3oxAhKyQ7wZifpDRFF3vbLM+al2wZO3R0RiCKATmuljXgAX9imUzfkSz7QUxnnLIsls2w73IMVY/pezfyfAsceMBjP3JNin9XQ3jC3KZKEuDtKkigBY1Me5GsHs4Ocb/KRd8Psok
9V+butL0nzJ/9bHYIh8cz6uxeRbttC/+YbnzW5+JOXs5ePtQu9FxhOlLD2rxghGmLLQQz3Qtdfjj5QGFTiWwEn7JfT+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.

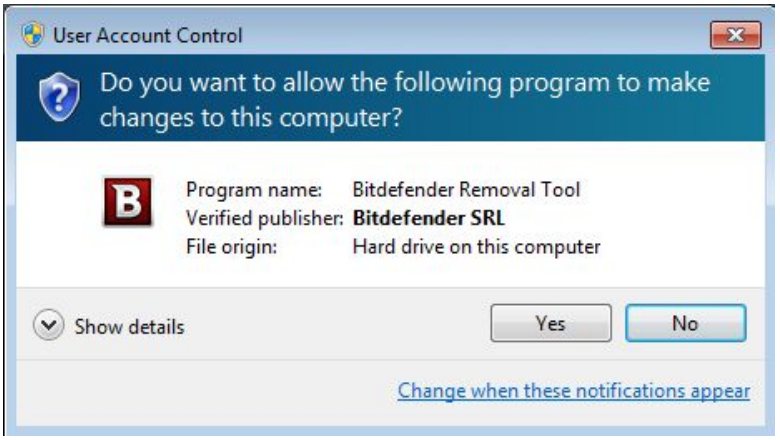


Steps for decryption:

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.*

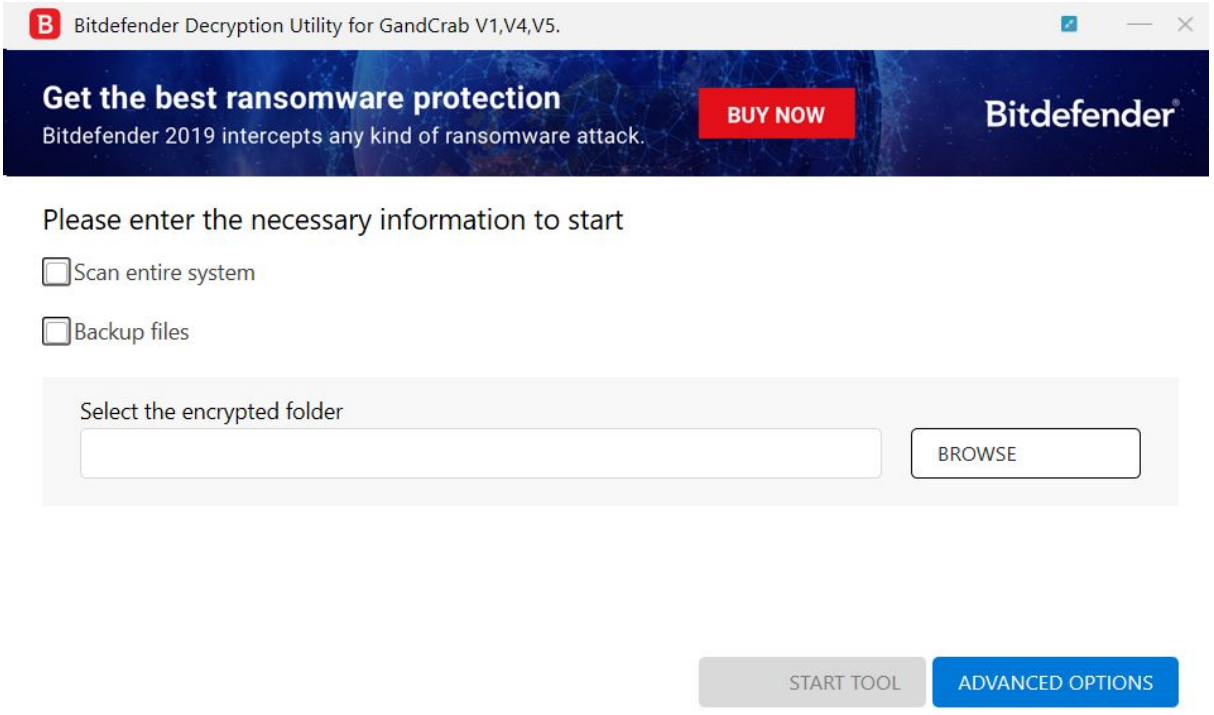
Step 2: Double-click the file (previously saved as BDGandCrabDecryptor.exe) and allow it to run by clicking Yes in the UAC prompt.



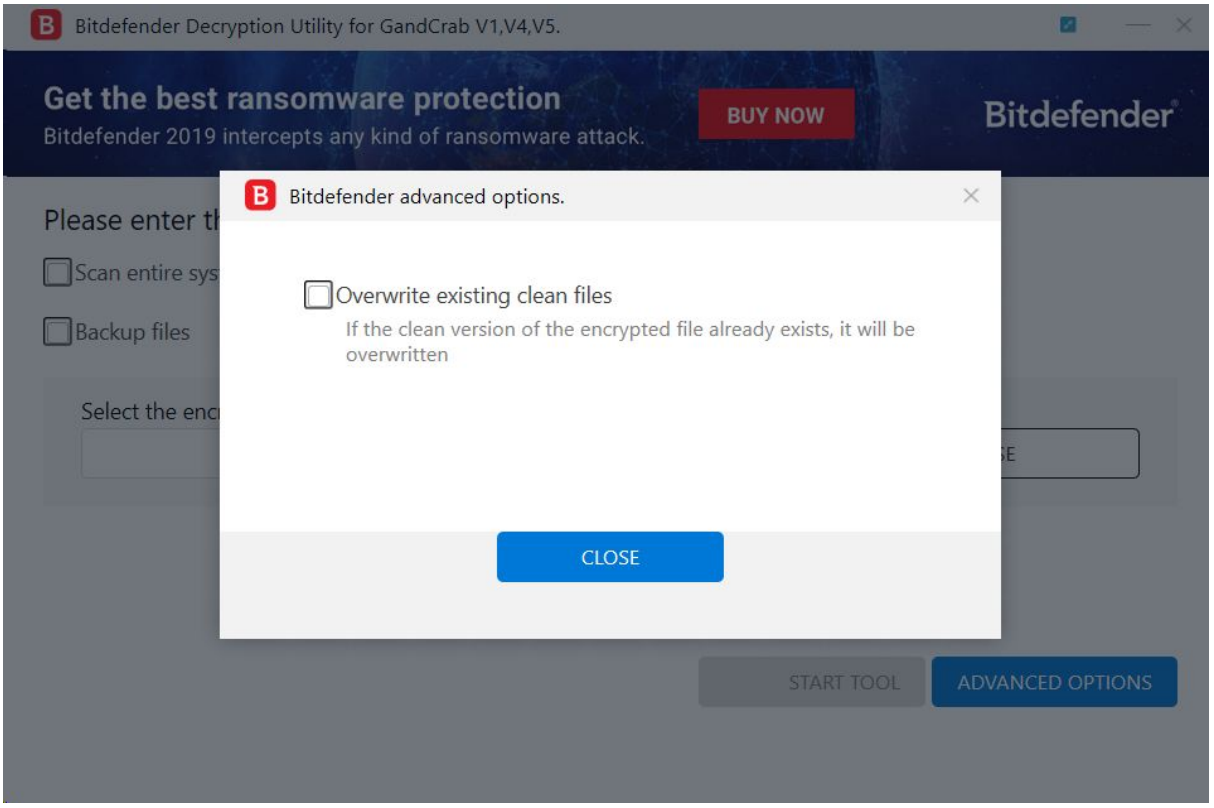
Step 3: Select “I Agree” for the End User License Agreement

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”.



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 encurage 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/)