GANDCRAB RANSOMWARE DECRYPTION TOOL

Introduction: This tool decrypts files encrypted by GandCrab ransomware. You can recognize this ransomware by the extension it appends to the encrypted files: (.GDCB).:

file1.docx.GDCB

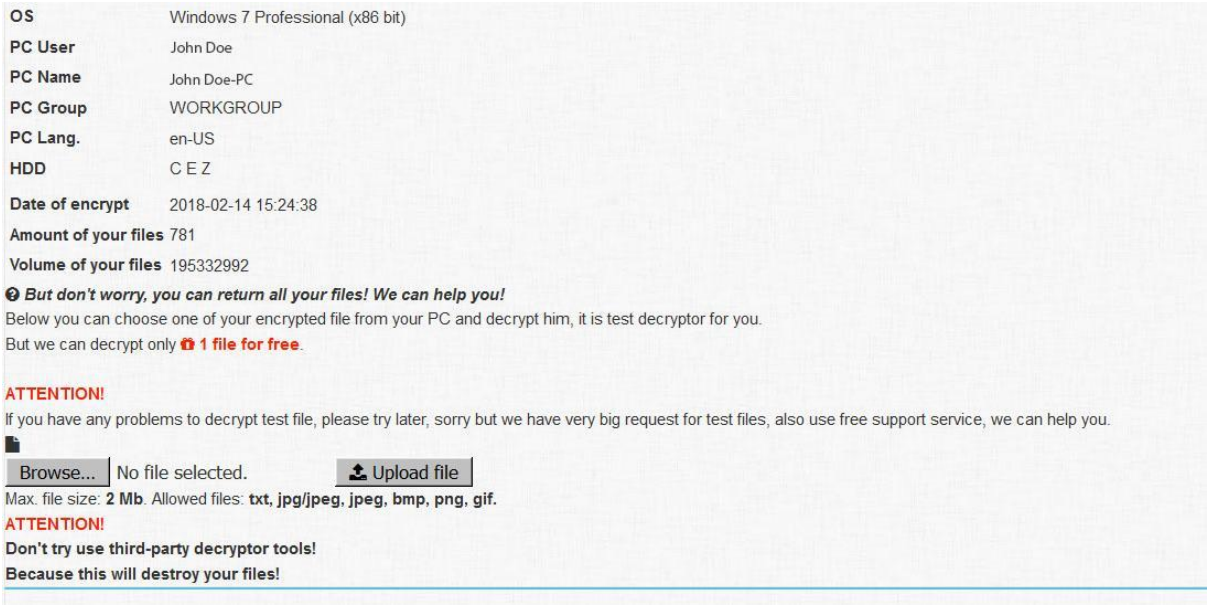
Tool is available for download at the following address:
http://download.bitdefender.com/am/malware_removal/BDGandCrabDecryptTool.exe
However, before using it, you need to ensure that you still have at least 1 ransom-note present on the PC containing your unique user_id:

Ransom-note: **C:\GDCB-DECRYPT.txt**

```
---= 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/user_id
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/user_id
2. http://gdcbghvjyqy7jclk.onion.casa/user_id
3. http://gdcbghvjyqy7jclk.onion.guide/user_id
4. http://gdcbghvjyqy7jclk.onion.rip/user_id
5. http://gdcbghvjyqy7jclk.onion.plus/user_id

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 encrypts user files using random AES256-CBC keys for each file, stored RSA-2048 encrypted at the end of the file.

Personal URL page content:



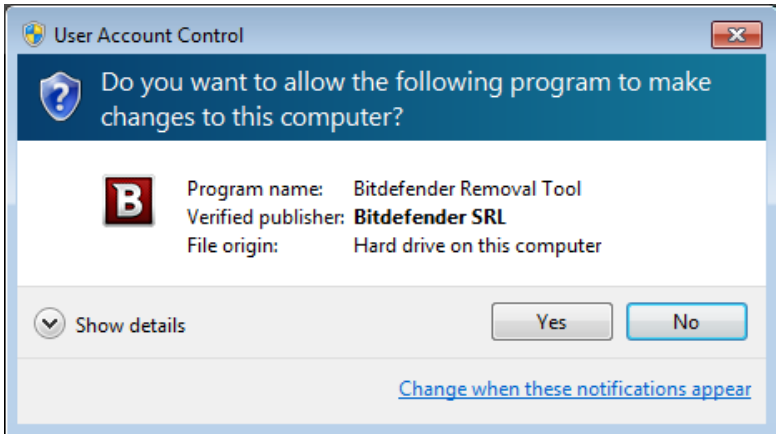
Example of encrypted files:

Steps for decryption:

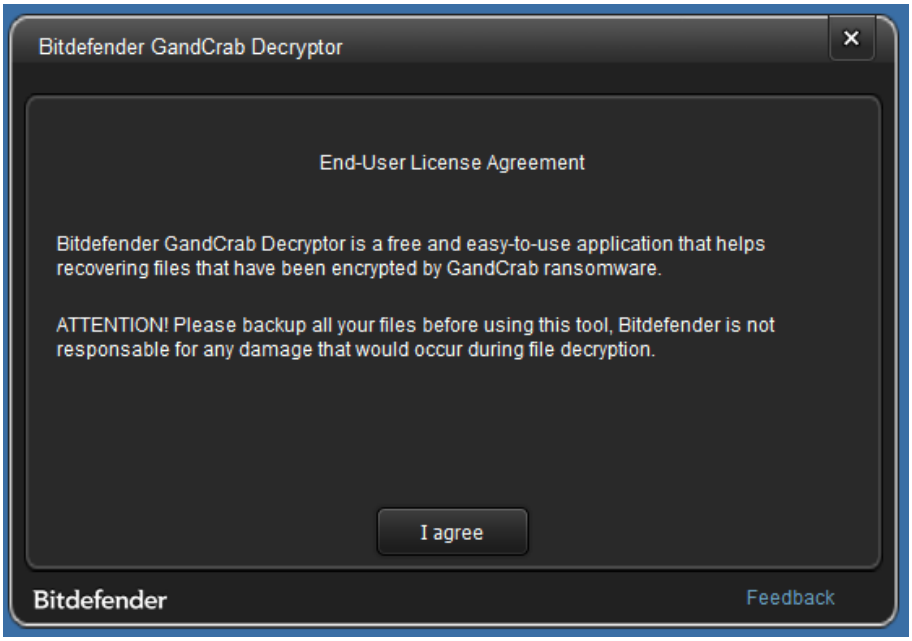
Step 1: Download the decryption tool and save it somewhere on your computer from: http://download.bitdefender.com/am/malware_removal/BDGandCrabDecryptor.exe

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

Step 2: Double click BDGandCrabDecryptor.exe and allow it to run by clicking yes on the UAC alert.

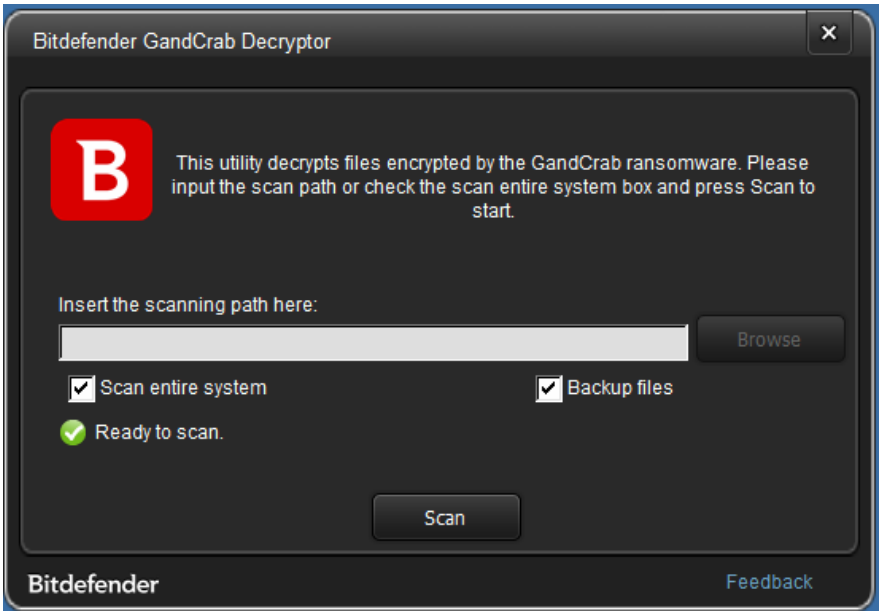


Step 3: Select "I Agree" for the End User License Agreement



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, should anything occur while decrypting. Then press “Scan”.

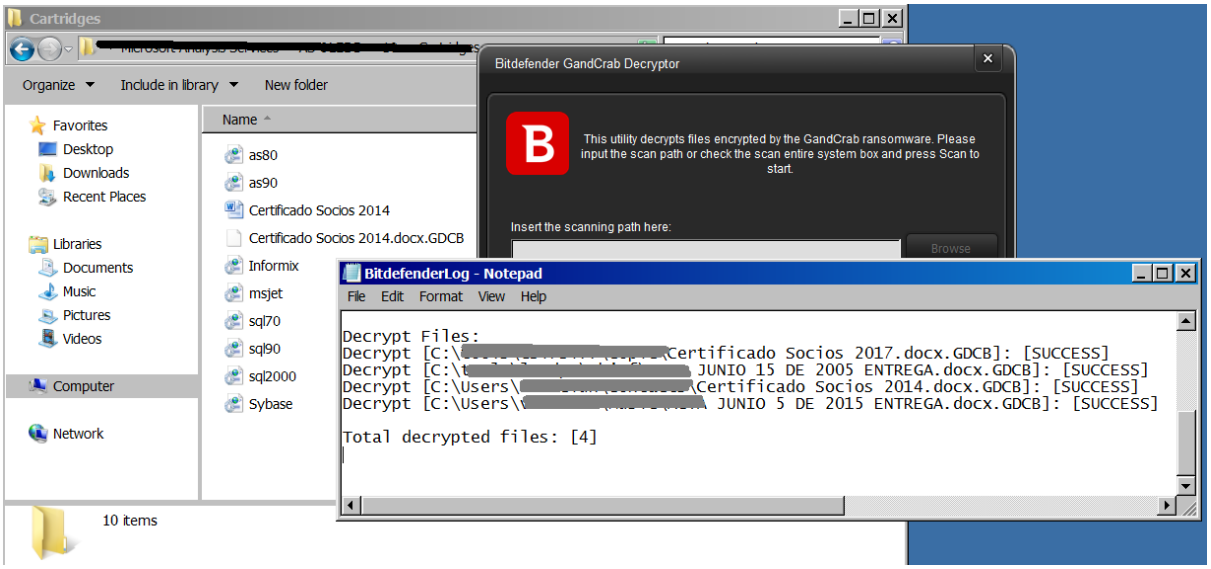


Regardless of whether you check the “Backup files” option ir not, the decryption tool attepmpts to decrypt 5 random files in the provided path and will NOT continue if the test is not successfully.

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 be presented with both the encrypted and decrypted files.

You can also find a log describing decryption process, in **%temp%\BDRemovalTool** folder:



Acknowledgement:

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