GoGoogle Decryption Tool

labs.bitdefender.com/2020/05/gogoogle-decryption-tool/

Bitdefender

May 07, 2020

One product to protect all your devices, without slowing them down.
Free 90-day trial

Bitdefender
Free ransomware decryption tools for business and home users
DOWNLOAD NOW

We’re happy to announce the availability of a new decryptor for GoGoogle (aka BossiTossi) ransomware. This family of ransomware is written in Go and generates encrypted files with the .google extension.

Spotted in April 2020, GoGoogle ransomware has several peculiarities.

First of all, it is written in Golang, a programming language that has grown popular among ransomware creators as of late. Secondly, the two versions of GoGoogle use two distinct encryption methods, depending on the size of the files to be encrypted. While one version exclusively uses XOR-based encryption, the other uses XOR for files larger than 1MB and RSA 1024 for smaller files.

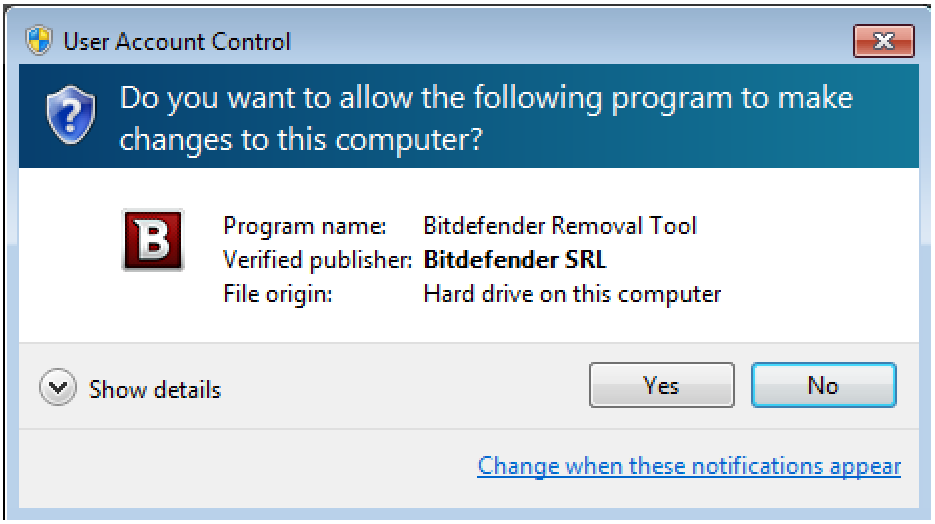
This decryptor currently solves infections for .google files encrypted with the XOR method. An updated decryptor to become available in the future will handle the RSA 1024 scenario as well.

How to use this tool

Step 1: Download the decryption tool below and save it on your computer.

Download the GoGoogle decryptor

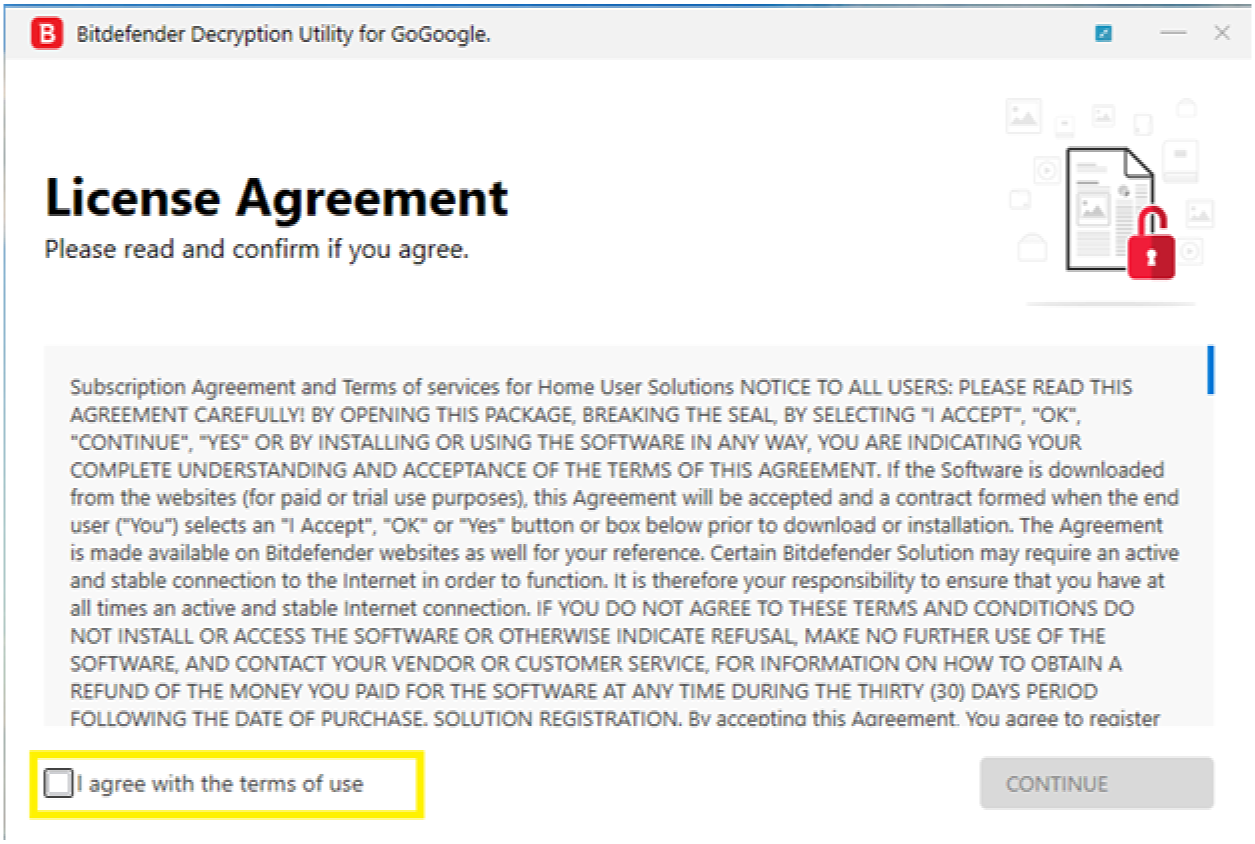
Step 2: Double-click the file (previously saved as BDGoGoogleDecryptor.exe) and allow it to run.


User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Bitdefender Removal Tool
Verified publisher: Bitdefender SRL
File origin: Hard drive on this computer

Step 3: Select “I Agree” in the License Agreement screen



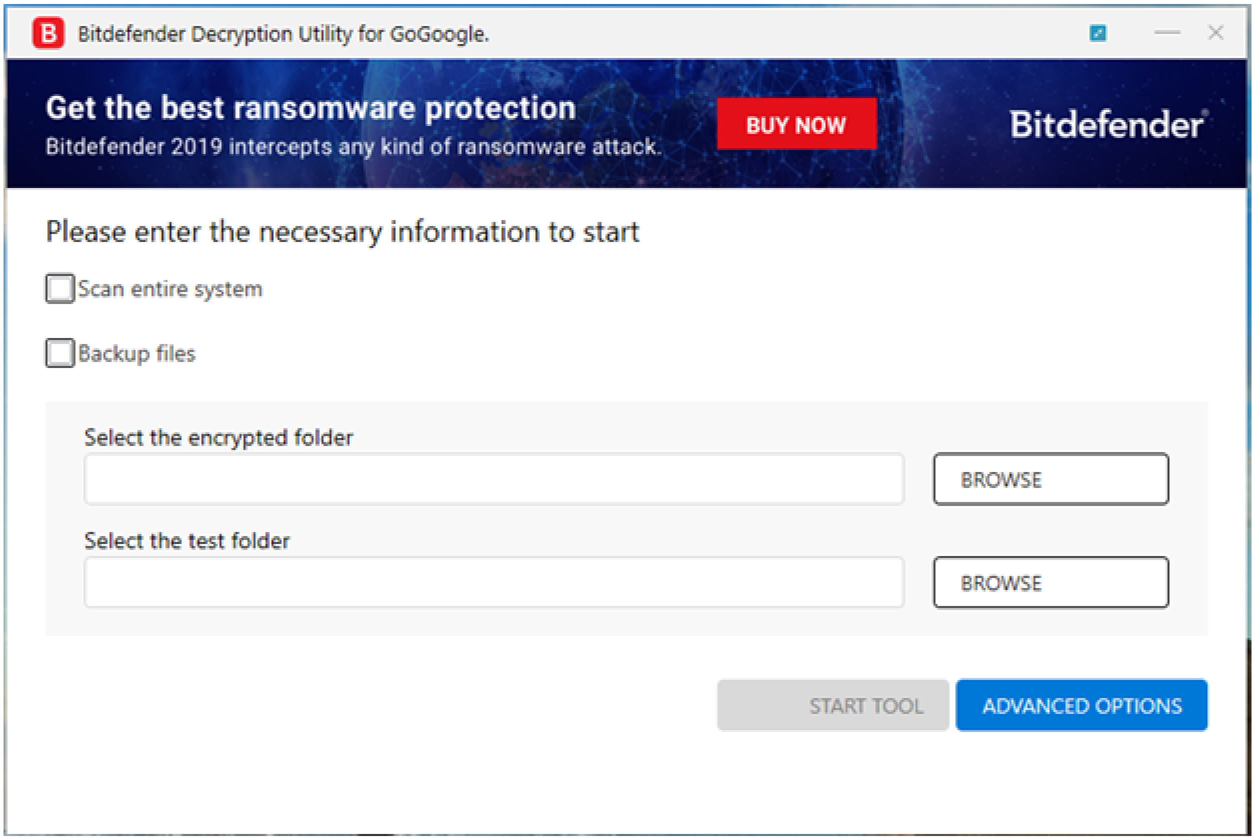
License Agreement

Please read and confirm if you agree.

Subscription Agreement and Terms of services for Home User Solutions NOTICE TO ALL USERS: PLEASE READ THIS AGREEMENT CAREFULLY! BY OPENING THIS PACKAGE, BREAKING THE SEAL, BY SELECTING "I ACCEPT", "OK", "CONTINUE", "YES" OR BY INSTALLING OR USING THE SOFTWARE IN ANY WAY, YOU ARE INDICATING YOUR COMPLETE UNDERSTANDING AND ACCEPTANCE OF THE TERMS OF THIS AGREEMENT. If the Software is downloaded from the websites (for paid or trial use purposes), this Agreement will be accepted and a contract formed when the end user ("You") selects an "I Accept", "OK" or "Yes" button or box below prior to download or installation. The Agreement is made available on Bitdefender websites as well for your reference. Certain Bitdefender Solution may require an active and stable connection to the Internet in order to function. It is therefore your responsibility to ensure that you have at all times an active and stable Internet connection. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS DO NOT INSTALL OR ACCESS THE SOFTWARE OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE, AND CONTACT YOUR VENDOR OR CUSTOMER SERVICE, FOR INFORMATION ON HOW TO OBTAIN A REFUND OF THE MONEY YOU PAID FOR THE SOFTWARE AT ANY TIME DURING THE THIRTY (30) DAYS PERIOD FOLLOWING THE DATE OF PURCHASE. SOLUTION REGISTRATION. By accepting this Agreement, You agree to register

☐ I agree with the terms of use

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


Bitdefender Decryption Utility for GoGoogle.

Please enter the necessary information to start

□ Scan entire system

□ Backup files

Select the encrypted folder

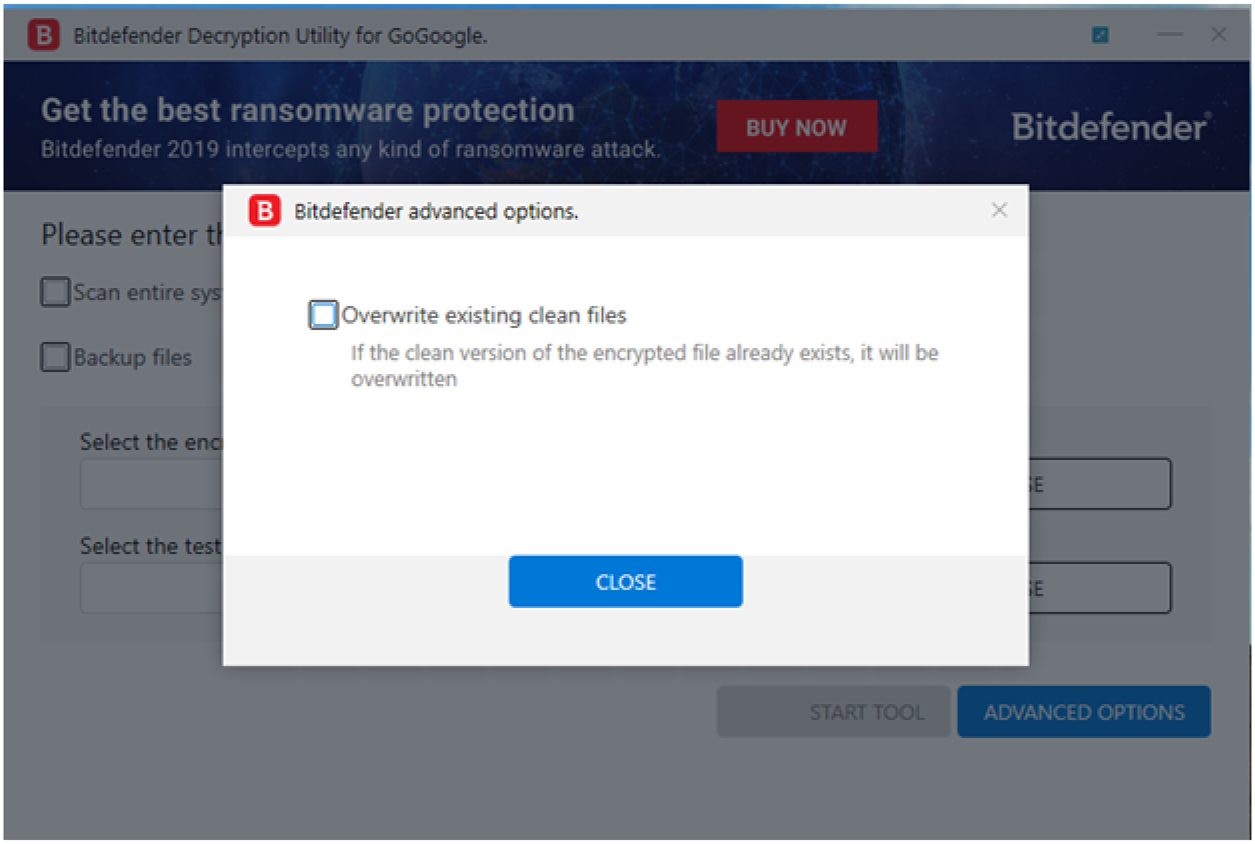
Select the test folder

Get the best ransomware protection
Bitdefender 2019 intercepts any kind of ransomware attack.
BUY NOW
Bitdefender
BROWSE
BROWSE
START TOOL
ADVANCED OPTIONS

The “test folder” must contain two pairs of original/encrypted files which will be used to determine the decryption type. It is essential that this folder only contains two pairs:

-1 pair of encrypted/original files, both smaller than 1 MB.
-1 pair of encrypted/original files, both larger than 2 MB.
NOTE: Some versions of GoGoogle are known for irrecoverably altering files under 2MB.

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.



Bitdefender Decryption Utility for GoGoogle.
Get the best ransomware protection
Bitdefender 2019 intercepts any kind of ransomware attack.
BUY NOW
Bitdefender
Please enter t
Scan entire sys
Backup files
Select the enc
Select the test
START TOOL
ADVANCED OPTIONS
Bitdefender advanced options.
CLOSE

□ Overwrite existing clean files

If the clean version of the encrypted file already exists, it will be overwritten

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

- -help - provides 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
- -test - this argument specifies the test path where should be a pair of original/encrypted files
- o0:1 - enables Scan entire system option (ignoring -path argument)
- o1:1 - enables Backup files option
- o2:1 - enables Overwrite existing files option

Examples:

BDGoGoogleDecryptor.exe start -path:"C:\" -> the tool starts with no GUI and scan C:\
BDGoGoogleDecryptor.exe start o0:1 -> the tool starts with no GUI and scan entire system
BDGoGoogleDecryptor.exe start o0:1 o1:1 o2:1 -> the tool scans 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/)

TAGS

anti-malware research   free tools

AUTHOR

hical

rp eye.”