

# RotorCrypt (RotoCrypt) Ransomware Support Topic - .tar, .c400, .c300, .GRANIT

---

[bleepingcomputer.com/forums/t/629699/rotorcrypt-rotocrypt-ransomware-support-topic-tar-c400-c300-granit/](https://bleepingcomputer.com/forums/t/629699/rotorcrypt-rotocrypt-ransomware-support-topic-tar-c400-c300-granit/)

## Advanced

Register a free account to unlock additional features at BleepingComputer.com

Welcome to **BleepingComputer**, a free community where people like yourself come together to discuss and learn how to use their computers. Using the site is easy and fun. As a guest, you can browse and view the various discussions in the forums, but can not create a new topic or reply to an existing one unless you are logged in. Other benefits of registering an account are subscribing to topics and forums, creating a blog, and having **no ads** shown anywhere on the site.

**[Click here to Register a free account now!](#)** or read our **[Welcome Guide](#)** to learn how to use this site.

**Latest News:** [Microsoft: The new Windows 11 features from Build 2022](#)

**Featured Deal:** [Shoot 4K from high angles with this two-pack of drones deal](#)



Started by Y2Breeze , Oct 17 2016 12:06 PM

Please log in to reply

23 replies to this topic

**#1**  **Y2Breeze**

---



- Members
- 5 posts
- OFFLINE

Local time:09:36 PM

Posted 17 October 2016 - 12:06 PM. (2016-10-17T13:06:31-04:00)

Hi

A client of mine got infected by something that looks like the Gomasom ransomware, but the end files are all in \*.tar

Here are 2 zip files, one with crypted files and the other with the same file from and old offline backup.

Any idea how to decrypt this?

[hxxp://datatest.simonznet.com/RANSOMWARE/](http://datatest.simonznet.com/RANSOMWARE/)

Thanks

Olivier

[↑ Back to top](#)

---

**BC AdBot (Login to Remove)**

---



- [BleepingComputer.com](#)
- [Register to remove ads](#)

---

## #2 Y2Breeze

---

- Topic Starter



- Members
- 5 posts
- OFFLINE

Local time:09:36 PM

Posted 17 October 2016 - 12:08 PM (2016-10-17T13:08:30-04:00)

There was no instruction for decrypt left on the computer. I wrote to the email using a random email and here is their answer

**Good day**

**Your files were encrypted/locked**

**As evidence can decrypt file 1 to 3 1-30MB**

**The price of the transcripts of all the files on the server: 7 Bitcoin**

**Recommend to solve the problem quickly and not to delay**

**Also give advice on how to protect Your server against threats from the network**

**(Files sql mdf backup decryption strictly after payment)!**

[↑ Back to top](#)

### #3 \_quietman7

---

Bleepin' Gumshoe

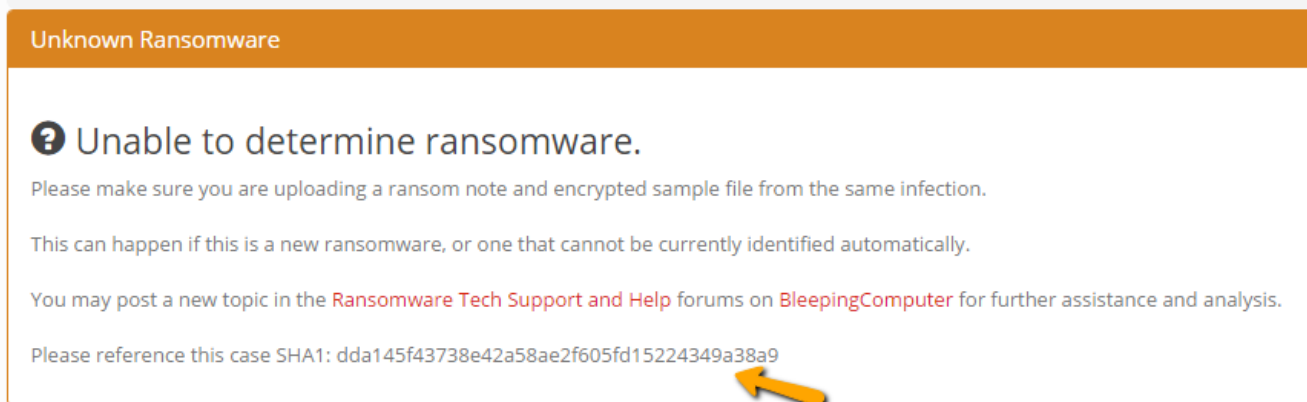


- Global Moderator
- 59,525 posts
- ONLINE
  
- Gender:Male
- Location:Virginia, USA
- Local time:09:36 PM

Posted 17 October 2016 - 12:33 PM (2016-10-17T13:33:23-04:00)

You can submit samples of encrypted files and ransom notes to **ID Ransomware** for assistance with identification and confirmation. This is a service that helps identify what ransomware may have encrypted your files and then attempts to direct you to an appropriate support topic where you can seek further assistance. Uploading both encrypted files and ransom notes together provides a more positive match and helps to avoid false detections. If ID Ransomware cannot identify the infection, you can post the **case SHA1** it gives you for [Demonslay335](#) to manually inspect the files.

Example screenshot:



Windows Insider MVP 2017-2020

Microsoft MVP Reconnect 2016

Microsoft MVP Consumer Security 2007-2015 

Member of [UNITE](#), Unified Network of Instructors and Trusted Eliminators

If I have been helpful & you'd like to consider a donation, click 

[↑ Back to top](#)

---

#### #4 [quietman7](#)

---

Bleepin' Gumshoe



- Global Moderator
- 59,525 posts
- ONLINE
  
- Gender:Male
- Location:Virginia, USA
- Local time:09:36 PM

Posted 17 October 2016 - 12:33 PM (2016-10-17T13:33:43-04:00)

Samples of any encrypted files, ransom notes or suspicious executables (installer, malicious files, attachments) that you suspect were involved in causing the infection can be submitted [here](http://www.bleepingcomputer.com/submit-malware.php?channel=168) (<http://www.bleepingcomputer.com/submit-malware.php?channel=168>) with a link to this topic. Doing that will be helpful with analyzing and investigating by our crypto experts.

**Windows Insider MVP 2017-2020**

**Microsoft MVP Reconnect 2016**

Microsoft MVP Consumer Security 2007-2015 

Member of [UNITE](#), Unified Network of Instructors and Trusted Eliminators

If I have been helpful & you'd like to consider a donation, click 

[↑ Back to top](#)

---

## #5 Y2Breeze

---

- Topic Starter



- Members
- 5 posts
- OFFLINE

Local time:09:36 PM

Posted 17 October 2016 - 12:39 PM (2016-10-17T13:39:28-04:00)

ID Ransomware cannot identify the ransomware.

SHA1 is fd65d1e0b248c8ec254ab3086f5877ff2065d72a

Sending the files to your second link right now.

[↑ Back to top](#)

---

## #6 quietman7

---

Bleepin' Gumshoe



- Global Moderator
  - 59,525 posts
  - ONLINE
- 
- Gender:Male
  - Location:Virginia, USA
  - Local time:09:36 PM

Posted .17.October.2016.-.02:58.PM.(2016-10-17T15:58:25-04:00)

Ok.

After our experts examine the files, they will post in this topic if they can assist or need further information.

.  
.

**Windows Insider MVP 2017-2020**

**Microsoft MVP Reconnect 2016**

**Microsoft MVP Consumer Security 2007-2015**



Member of UNITE, Unified Network of Instructors and Trusted Eliminators

If I have been helpful & you'd like to consider a donation, click [Donate](#)

[↑ Back to top](#)

---

**#7** [←\\_mike](#) 1

---



- Members
  - 210 posts
  - OFFLINE
- 
- Gender:Male
  - Location:Russia, Moscow
  - Local time:05:36 AM

Posted .17.October.2016.-.03:21.PM.(2016-10-17T16:21:55-04:00)

This is Trojan-Ransom.Win32.Rotor.

Sample: <https://www.hybrid-analysis.com/sample/e4a60a227edaff8c43cf1b318f45e70d23fa5c068fb5d578cb8aeb87358866f6?environmentId=100>

VT: <https://www.virustotal.com/ru/file/e4a60a227edaff8c43cf1b318f45e70d23fa5c068fb5d578cb8aeb87358866f6/analysis/>

Мы разные, но идея одна!

[↑ Back to top](#)

---

## #8 [← SamsonFromTheBible](#)

---



- Members
- 11 posts
- OFFLINE
  
- Gender:Male
- Local time:03:36 AM

Posted 18 October 2016 - 05:09 AM (2016-10-18T06:09:19-04:00)

Is the virus on Mac by any chance?

[↑ Back to top](#)

---

## #9 [← Y2Breeze](#)

---

- Topic Starter



- Members
- 5 posts
- OFFLINE



Local time:09:36 PM

Posted 18 October 2016 - 10:03 AM. (2016-10-18T11:03:27-04:00)

No, Windows 7

[↑ Back to top](#)

---

## #10 [← Demonslay335](#)

---

Ransomware Hunter



- Security Colleague
- 4,748 posts
- OFFLINE
  
- Gender:Male
- Location:USA
- Local time:07:36 PM


Posted 18 October 2016 - 06:54 PM. (2016-10-18T19:54:09-04:00)

Interesting, I have not seen a ransomware use ".tar". It isn't a valid Tar archive either. Can you also upload the ransom note to ID Ransomware so I can archive it?

Thanks for the sample mike1. Has any further analysis been done on it already? It crashed on my VM. I see RakhniDecryptor lists it, but it stated unsupported when I selected this user's files.

**Edited by Demonslay335, 18 October 2016 - 06:55 PM.**

 [ID Ransomware](#) - Identify What Ransomware Encrypted Your Files [[Support Topic](#)]

 [RansomNoteCleaner](#) - Remove Ransom Notes Left Behind [[Support Topic](#)]

 [CryptoSearch](#) - Find Files Encrypted by Ransomware [[Support Topic](#)]

If I have helped you and you wish to support my ransomware fighting, you may support me [here](#).

[↑ Back to top](#)

---

## #11 [↩](#) \_Y2Breeze

---

- Topic Starter



- Members
- 5 posts
- OFFLINE

Local time:09:36 PM

Posted 20 October 2016 - 11:56 AM. (2016-10-20T12:56:47-04:00)

There is no ransom note anywhere. All we figure out was to try to write to the email Embedded in encrypted files filename.

[↑ Back to top](#)

---

## #12 [↩](#) \_mike 1

---



- Members
- 210 posts
- OFFLINE

- Gender:Male
- Location:Russia, Moscow
- Local time:05:36 AM

Posted 21 October 2016 - 05:10 AM. (2016-10-21T06:10:37-04:00)

Thanks for the sample mike1. Has any further analysis been done on it already? It crashed on my VM. I see RakhniDecryptor lists it, but it stated unsupported when I selected this user's files.

Tech support at Kaspersky Lab said that can not decrypted.

Мы разные, но идея одна!

[↑ Back to top](#)

---

## #13 [← mike 1](#)

---



- Members
- 210 posts
- OFFLINE

- Gender:Male
- Location:Russia, Moscow
- Local time:05:36 AM

Posted 31 October 2016 - 10:23 AM. (2016-10-31T11:23:17-04:00)

<https://www.virustotal.com/ru/file/b20177fa76cc97cfb9d6d7425d636ade46980420ca1d8b5f8b662d4ba8cb1ba8/analysis/>

Rotocrypt. Variant \_\_\_ELIZABETH7@PROTONMAIL.COM\_\_\_crypt

Мы разные, но идея одна!

[↑ Back to top](#)

---

## #14 jumpline

---



- Members
- 4 posts
- OFFLINE

- Gender:Male
- Location:Russia, Moscow
- Local time:04:36 AM

Posted 03.November.2016.-.05:02.AM.(2016-11-03T06:02:29-04:00)

Hello, can someone help with a decoder? It encrypts all files

!\_\_\_\_LIKBEZ77777@GMAIL.COM\_\_\_\_.c400

Below are links to a virus and a link to the encrypted file.

<http://www.filedropper.com/viruspass123> (password 123)

<http://www.filedropper.com/perenosdannihxmllikbez77777gmailcom>

[↑ Back to top](#)

---

## #15 quietman7

---

Bleepin' Gumshoe



- Global Moderator
- 59,525 posts
- ONLINE

- Gender:Male
- Location:Virginia, USA
- Local time:09:36 PM

Posted 03 November 2016 - 05:50 AM. (2016-11-03T06:50:52-04:00)

You can submit samples of encrypted files and ransom notes to **ID Ransomware** for assistance with identification and confirmation. This is a service that helps identify what ransomware may have encrypted your files and then attempts to direct you to an appropriate support topic where you can seek further assistance. Uploading both encrypted files and ransom notes together provides a more positive match and helps to avoid false detections.

**Windows Insider MVP 2017-2020**

**Microsoft MVP Reconnect 2016**

**Microsoft MVP Consumer Security 2007-2015**



Member of **UNITE**, Unified Network of Instructors and Trusted Eliminators

If I have been helpful & you'd like to consider a donation, click 

[↑ Back to top](#)

---

[Back to Ransomware Help & Tech Support](#)

**0 user(s) are reading this topic**

0 members, 0 guests, 0 anonymous users

[Community Forum Software by IP.Board](#)