

[Create Request](#) | [Personal Account](#)[SOLUTIONS](#) [RENEW](#) [DOWNLOADS](#) [SUPPORT](#) [RESOURCE CENTER](#) [PARTNERS](#) [ABOUT KASPERSKY LAB](#)

English (Global) ▼

[Home](#) → [Support](#) → Safety 101[Product Select](#) [Sources of threats](#) [Types of threats](#) [Signs of infection](#) [General information](#) [PC Safety](#) [Virus-fighting utilities](#) [Viruses and solutions](#)

Safety 101: Virus-fighting utilities

RakhniDecryptor tool for removing Trojan-Ransom.Win32.Rakhni malicious software (.oshit and others)

[Back to "Virus-fighting utilities"](#)

2018 Feb 14 ID: 10556

Use the [RakhniDecryptor.zip](#) to decrypt your files in case they are encrypted by the following types of malware:

- Trojan-Ransom.Win32.Rakhni
- Trojan-Ransom.Win32.Agent.iih
- Trojan-Ransom.Win32.Autoit
- Trojan-Ransom.Win32.Aura
- Trojan-Ransom.AndroidOS.Pletor
- Trojan-Ransom.Win32.Rotor
- Trojan-Ransom.Win32.Lamer
- Trojan-Ransom.Win32.Cryptokluchen
- Trojan-Ransom.Win32.Democry
- Trojan-Ransom.Win32.Bitman version 3 and 4
- Trojan-Ransom.Win32.Libra
- Trojan-Ransom.MSIL.Lobzik
- Trojan-Ransom.MSIL.Lortok
- Trojan-Ransom.Win32.Chimera
- Trojan-Ransom.Win32.CryFile
- Trojan-Ransom.Win32.Nemchig
- Trojan-Ransom.Win32.Mircop
- Trojan-Ransom.Win32.Mor
- Trojan-Ransom.Win32.Crusis
- Trojan-Ransom.Win32.AecHu
- Trojan-Ransom.Win32.Jaff

- Trojan-Ransom.Win32.Cryakl CL 1.0.0.0
- Trojan-Ransom.Win32.Cryakl CL 1.0.0.0.u
- Trojan-Ransom.Win32.Cryakl CL 1.2.0.0
- Trojan-Ransom.Win32.Cryakl CL 1.3.0.0
- Trojan-Ransom.Win32.Cryakl CL 1.3.1.0

Files that can be decrypted with RakhniDecryptor

When malware encrypts files, it changes the file extensions. For example:

- before **file.doc** / after **file.doc.locked**
- before **1.doc** / after **1.dochb15**
- before **1.doc** / after **1.doc._17-05-2016-20-27-37_\$seven_legion@india.com\$.777**

The [RakhniDecryptor.zip](#) tool can decrypt the files encrypted according to the following templates:

Trojan-Ransom.Win32.Rakhni:

- <file_name>.<original_extension>.<locked>
- <file_name>.<original_extension>.<kraken>
- <file_name>.<original_extension>.<darkness>
- <file_name>.<original_extension>.<oshit>
- <file_name>.<original_extension>.<nochance>
- <file_name>.<original_extension>.<oplata@qq_com>
- <file_name>.<original_extension>.<relock@qq_com>
- <file_name>.<original_extension>.<crypto>
- <file_name>.<original_extension>.<helpdecrypt@ukr.net>
- <file_name>.<original_extension>.<pizda@qq_com>
- <file_name>.<original_extension>.<dyatel@qq_com>
- <file_name>.<original_extension>.<nalog@qq_com>
- <file_name>.<original_extension>.<chifrator@gmail_com>
- <file_name>.<original_extension>.<gruzin@qq_com>
- <file_name>.<original_extension>.<troyancoder@gmail_com>
- <file_name>.<original_extension>.<coderksu@gmail_com_id373>
- <file_name>.<original_extension>.<coderksu@gmail_com_id371>
- <file_name>.<original_extension>.<coderksu@gmail_com_id372>
- <file_name>.<original_extension>.<coderksu@gmail_com_id374>
- <file_name>.<original_extension>.<coderksu@gmail_com_id375>
- <file_name>.<original_extension>.<coderksu@gmail_com_id376>
- <file_name>.<original_extension>.<coderksu@gmail_com_id392>
- <file_name>.<original_extension>.<coderksu@gmail_com_id357>
- <file_name>.<original_extension>.<coderksu@gmail_com_id356>
- <file_name>.<original_extension>.<coderksu@gmail_com_id358>
- <file_name>.<original_extension>.<coderksu@gmail_com_id359>
- <file_name>.<original_extension>.<coderksu@gmail_com_id360>
- <file_name>.<original_extension>.<coderksu@gmail_com_id20>

Trojan-Ransom.Win32.Mor:

- <file_name>.<original_extension>_crypt

Trojan-Ransom.Win32.Autoit:

- <<file_name>.<original_extension>.<_crypt@india.com_.random characters>

Trojan-Ransom.MSIL.Lortok:

- <file_name>.<original_extension>.<cry>
- <file_name>.<original_extension>.<AES256>

Trojan-Ransom.AndroidOS.Pletor:

- <file_name>.<original_extension>.<enc>

Trojan-Ransom.Win32.Agent.iih:

- <file_name>.<original_extension>+<hb15>

Trojan-Ransom.Win32.CryFile:

- <file_name>.<original_extension>.<encrypted>

Trojan-Ransom.Win32.Democry:

- <file_name>.<original_extension>+<._date-time_\$email@domain\$.777>
- <file_name>.<original_extension>+<._date-time_\$email@domain\$.legion>

Trojan-Ransom.Win32.Bitman version 3:

- <file_name>.<xxx>
- <file_name>.<ttt>
- <file_name>.<micro>
- <file_name>.<mp3>

Trojan-Ransom.Win32.Bitman version 4:

- <file_name>.<original_extension> (file name and extension are not changed)

Trojan-Ransom.Win32.Libra:

- <file_name>.<encrypted>
- <file_name>.<locked>
- <file_name>.<SecureCrypted>

Trojan-Ransom.MSIL.Lobzik:

- <file_name>.<fun>
- <file_name>.<gws>
- <file_name>.<btc>
- <file_name>.<AFD>
- <file_name>.<porno>
- <file_name>.<pornoransom>
- <file_name>.<epic>
- <file_name>.<encrypted>
- <file_name>.<J>
- <file_name>.<payransom>
- <file_name>.<paybtcs>
- <file_name>.<paymds>
- <file_name>.<paymrss>
- <file_name>.<paymrts>
- <file_name>.<paymst>
- <file_name>.<paymts>
- <file_name>.<gefickt>

- <file_name>.<uk-dealer@sigaint.org>

Trojan-Ransom.Win32.Mircop:

- <Lock>.<file_name>.<original_extension>

Trojan-Ransom.Win32.Crusis:

- .ID<...>.<mail>@<server>.<domain>.xtbl
- .ID<...>.<mail>@<server>.<domain>.CrySiS
- .id-<...>.<mail>@<server>.<domain>.xtbl
- .id-<...>.<mail>@<server>.<domain>.wallet
- .id-<...>.<mail>@<server>.<domain>.dhrama
- .id-<...>.<mail>@<server>.<domain>.onion
- .<mail>@<server>.<domain>.wallet
- .<mail>@<server>.<domain>.dhrama
- .<mail>@<server>.<domain>.onion

Trojan-Ransom.Win32. Nemchig:

- <file_name>.<original_extension>.<safefiles32@mail.ru>

Trojan-Ransom.Win32.Lamer:

- <file_name>.<original_extension>.<bloked>
- <file_name>.<original_extension>.<cripaaaa>
- <file_name>.<original_extension>.<smit>
- <file_name>.<original_extension>.<fajlovnet>
- <file_name>.<original_extension>.<filesfucked>
- <file_name>.<original_extension>.<criptx>
- <file_name>.<original_extension>.<gopaymeb>
- <file_name>.<original_extension>.<cripted>
- <file_name>.<original_extension>.<bnmntftfmn>
- <file_name>.<original_extension>.<criptiks>
- <file_name>.<original_extension>.<cripttt>
- <file_name>.<original_extension>.<hithere>
- <file_name>.<original_extension>.<aga>

Trojan-Ransom.Win32.Cryptokluchen:

- <file_name>.<original_extension>.<AMBA>
- <file_name>.<original_extension>.<PLAGUE17>
- <file_name>.<original_extension>.<ktldll>

Trojan-Ransom.Win32.Rotor:

- <file_name>.<original_extension>.<.-.DIRECTORAT1C@GMAIL.COM.oto>
- <file_name>.<original_extension>.<.-.CRYPTSb@GMAIL.COM.oto>
- <file_name>.<original_extension>.<.-.DIRECTORAT1C8@GMAIL.COM.oto>
- <file_name>.<original_extension>.<!_____DESKRYPTEDN81@GMAIL.COM.crypt>
- <file_name>.<original_extension>.<!____prosschiff@gmail.com_.crypt>
- <file_name>.<original_extension>.<!_____GASWAGEN123@GMAIL.COM____.crypt>
- <file_name>.<original_extension>.<!_____pkigxdaq@bk.ru____.crypt>
- <file_name>.<original_extension>.<!_____moskali1993@mail.ru____.crypt>
- <file_name>.<original_extension>.<!==helpsend369@gmail.com==.crypt>
- <file_name>.<original_extension>.<!==kronstar21@gmail.com==-.crypt>

Trojan-Ransom.Win32.Chimera:

- <file_name>.<original_extension>.<crypt>
- <file_name>.<original_extension>.<4 random characters>

Trojan-Ransom.Win32.AecHu:

- <file_name>.<aes256>
- <file_name>.<aes_ni>
- <file_name>.<aes_ni_gov>
- <file_name>.<aes_ni_0day>
- <file_name>.<lock>
- <file_name>.<decrypr_helper@freemail_hu>
- <file_name>.<decrypr_helper@india.com>
- <file_name>.<~xdata>

Trojan-Ransom.Win32.Jaff:

- <file_name>.<jaff>
- <file_name>.<wlu>
- <file_name>.<sVn>

Trojan-Ransom.Win32.Cryakl

- email-<...>.ver-<...>.id-<...>.randomname-<...>.<random_extension>

Malware version Email address

	cryptolocker@aol.com
	iizomer@aol.com
	seven_Legion2@aol.com
	oduvansh@aol.com
CL 1.0.0.0	ivanivanov34@aol.com
	trojanencoder@aol.com
	load180@aol.com
	moshiax@aol.com
	vpupkin3@aol.com
	watnik91@aol.com
	cryptolocker@aol.com_graf1
CL 1.0.0.0.u	cryptolocker@aol.com_mod
	byaki_buki@aol.com_mod2
	oduvansh@aol.com
CL 1.2.0.0	cryptolocker@aol.com

CL 1.3.0.0

cryptolocker@aol.com

byaki_buki@aol.com

CL 1.3.1.0

byaki_buki@aol.com_grafdrkula@gmail.com

vpupkin3@aol.com

How to use the tool

Parameters for running the utility from the command prompt

Was this information helpful?

[Yes](#) [No](#)

[Back to "Virus-fighting utilities"](#)

Support for Home

[Consumer Support Contacts](#)

[Contact support via My Kaspersky](#)

[Knowledge Base for Home](#)

[How-to Videos](#)

[Forum](#)

Virus-fighting tools & services

[Scan file or URL for viruses](#)

[Report a false alarm](#)

[Kaspersky Virus Removal Tool](#)

[Kaspersky Rescue Disk](#)

[Other virus-fighting tools](#)

Support for Small Business

[Small Business Support Contacts](#)
[Contact support via My Kaspersky](#)
[Knowledge Base for Small Business](#)
[Forum](#)

Software Downloads

[Buy online](#)
[Renew license](#)
[Get updates](#)
[Free trial download](#)

[Support terms and conditions](#)
(updated April 12, 2017)

Support for Business

[Business Support Contacts](#)
[Contact support via Company Account](#)
[Knowledge Base for Business](#)
[Product Support Lifecycle](#)
[Premium Support Plans](#)
[Licensing by Subscription](#)
[Forum](#)
[Online Trainings](#)
[Subscribe to news](#)

[Site Feedback](#)

© 2018 AO Kaspersky Lab. All Rights Reserved.


[Privacy Policy](#) [Contact Us](#) [About us](#)

•

-

Have you found what you were looking for?

Please let us know how we can make this website more comfortable for you

Enter your feedback here (max. 500)	
--	---

Send feedback [Send feedback](#)

Thank you!

Thank you for submitting your feedback.
We will review your feedback shortly.