

Forum:[Hack Forums](#)

Thread: [ransom](#)

12321 - May 8, 2017, 1:15 am

Hi!

anyone know how to get rid of this (without paying them!)Quote:*** ALL YOUR WORK AND PERSONAL FILES HAVE BEEN ENCRYPTED *

To decrypt your files you need to buy the special software. To recover data, follow the instructions! You can find out the details/ask questions in the chat:

[fgb45ft3pqamyji7.onion.to](#) (not need Tor)

[fgb45ft3pqamyji7.onion.cab](#) (not need Tor)

[fgb45ft3pqamyji7.onion.nu](#) (not need Tor)

You ID: #####

If the resource is not available for a long time, install and use the Tor-browser:

1. Run your Internet-browser
2. Enter or copy the address torproject.org/download/download-easy.html in the address bar of your browser and press key ENTER
3. On the site will be offered to download the Tor-browser, download and install it. Run.
4. Connect with the button "Connect" (if you use the English version)
5. After connection, the usual Tor-browser window will open
6. Enter or copy the address [fgb45ft3pqamyji7.onion](#) in the address bar of Tor-browser and press key ENTER
7. Wait for the site to load

If you have any problems installing or using, please visit the video tutorial youtube.com/watch?v=gOgh3ABju6Q

in the chat they giving you this:Quote:To decrypt your files you need to buy the special software – «Nemesis decryptor»

The cost of the decoder: 300 USD

Payment method: Bitcoin

Bitcoin Wallet: 154HVeXdQUTTHVMoiM2gdm5rUho7W4kxb1

// After payment you will receive an instruction, decoder software and private key.

INSTRUCTIONS:

1. It is necessary to register here - blockchain.info/wallet/new
2. Find online shop that sells Bitcoin (cryptocurrency) and replenish your wallet. Query: buy bitcoin (in google) or from the list below.

3. en.bitcoin.it/wiki/Help:FAQ (for newbies) *****

Online shop:

coincafe.com

localbitcoins.com

remitano.com

coinbase.com

buybitcoinworldwide.com
xmlgold.eu
cex.io
247exchange.com

they got my family photos just before backup... ?

5chn4pp - May 8, 2017, 1:20 am

Submit the note and a encrypted file to this site:

<https://id-ransomware.malwarehunterteam.com/>

Also please tell us what extension your encrypted files has.

12321 - May 8, 2017, 1:53 am

(May 8, 2017 01:20 AM)Satudarah Wrote: [\[CITE\]](#) Submit the note and a encrypted file to this siteit says This Quote:ransomware is decryptable!

Identified by

ransomnote_url: fgb45ft3pqamyji7.onion

and possible to use cry9, but

oi66.tiny pic.com/14abu6p.jpg

oi64.tiny pic.com/34jajoj.jpg (sorry can't post images, remove space in tiny_pic)

(May 8, 2017 01:20 AM)Satudarah Wrote: [\[CITE\]](#) Also please tell us what extension your encrypted files has.Rufus v2.14.1086.exe.id_#####_fgb45ft3pqamyji7.onion

- my id number for the ransom

5chn4pp - May 8, 2017, 2:11 am

Try using a larger file than the one you used there, then post results.

12321 - May 8, 2017, 2:28 am

it wants differences between files 68b

and my files ~36b

5chn4pp - May 8, 2017, 4:31 am

Try these decryptors and see if it does anything:

<https://decrypter.emsisoft.com/cry9>

<https://decrypter.emsisoft.com/cry128>

Ranger. - May 8, 2017, 4:38 am

You should seek out real professional advice from someone such as a malware researcher.

If it turns out that the data cannot be decrypted & retrieved, due to the way that is coded then there is nothing that you can do.

Most of the ransom-ware nowadays are pretty secure and it should be pretty hard to retrieve the data, unless you're in a special case with a complete idiot of a programmer; if someone has done research on the piece of ransom-ware that infected you and it can be easily decrypted due to flaws in code.

If the family photos are really important for you and for your family then just pay the ransom. \$300 is a lot, I get it, but you will still end up wasting a lot by trying to find out if the data can be decrypted (through e.g. sending the PC to repair shops.)
And let me not mention the time that you will lose by trying to solve the issue..

12321 - May 8, 2017, 6:45 am

@Satudarah

i already tried almost all emsisoft tools, they heard about this malware version and on their forum they are talked about started working on the solution with crypton/cry9/cry128... but they don't know how long it will take...

@Ranger.

the problem with paying ransom is will i get files back or they just ruined them and want money, or will just take money and then what keep waiting in the stupid chat that they opened?

5chn4pp - May 8, 2017, 6:47 am

If you pay, theres like a 85% chance of getting your files back.

How did you get infected in the first place? Do you still have the file?

12321 - May 8, 2017, 6:54 am

i have no idea how it happened, there was random resets last week or two and yesterday after reset got this surprise...

how do i find out if it's still around or some timers waiting to "finish the job"?

5chn4pp - May 8, 2017, 7:15 am

What about this one:

<https://decrypter.emsisoft.com/crypton>

Also, please upload an encrypted file and post it here so i can look closer.

12321 - May 8, 2017, 7:36 am

yes
emsisoft have only 3 potential tools for this problem that they are working on their update
crypton/cry9/cry128

original:

upload.ee/files/6989190/SpeedyFox_v2.0.20.117.zip.html

changed:

upload.ee/files/6989192/SpeedyFox_v2.0.20.117.zip.id_188510917_fgb45ft3pqamyji7.onion.html

if it'll help more, i also have NFO files, maybe it'll be easier to find how they did it:

original:

upload.ee/files/6989228/uTorrent_-_Remove_Ads.nfo.html

changed:

upload.ee/files/6989229/uTorrent_-_Remove_Ads.nfo.id_188510917_fgb45ft3pqamyji7.onion.html

5chn4pp - May 8, 2017, 7:56 am

I can't get anything off them, all you can do now is either wait or pay sadly.

<https://www.bleepingcomputer.com/forums/t/646173/emergency-need-help-about-onion-virus/>

Also, it looks like this guy has the exactly same infection as you, so if you feel lucky you can lurk this thread to see if they find a way to decrypt.

12321 - May 8, 2017, 7:59 am

thanks! will add it to emsisoft's forum links...

if anyone else have this crap, this is the links i found:

[bleepingcomputer.com/forums/t/646173/emergency-need-help-about-onion-virus/](https://www.bleepingcomputer.com/forums/t/646173/emergency-need-help-about-onion-virus/) - thanks to Satudarah

[bleepingcomputer.com/forums/t/645847/unable-to-determine-ransomware-files-crypted/](https://www.bleepingcomputer.com/forums/t/645847/unable-to-determine-ransomware-files-crypted/)

[bleepingcomputer.com/forums/t/635859/crypton-ransomware-support-help-topic-id-number-x3m-locked-r9oj/page-10](https://www.bleepingcomputer.com/forums/t/635859/crypton-ransomware-support-help-topic-id-number-x3m-locked-r9oj/page-10)

support.emsisoft.com/topic/27231-cry9-invalid-crypton-file-pair/

Nickname. - May 14, 2017, 3:52 pm

Same issue! Any update? My RDP got hit by the Ransom none of Emisoft decrypters seemt too work!

12321 - May 15, 2017, 11:26 pm

no... :(

only to follow their progress with the links in post 14

EthanX - May 16, 2017, 6:11 pm

(May 14, 2017 03:52 PM)Nickname. Wrote: [\[CITE\]](#) Same issue! Any update? My RDP got hit by the Ransom none of Emisoft decrypters seemt too work!

What did you and OP do to get ransomware?

12321 - May 16, 2017, 11:48 pm

no idea... they telling you how to remove and fix the "door" only after you pay...

but emsisoft saying: it appears that all variants of the CryptON ransomware (such as Cry9/Cry128 ransomware) are infecting systems via RDP (remote desktop services) brute force attacks, which allows them to log into the victim's server and execute the ransomware.

and i saw the key from someone who paid it's 1-F, around 700 symbols...

Quote:ID: 2529633506

KEY:

323532393633333530365F98797F971922B5AFF47E3DB0590CD47F3BCBE7F89CF79457757C6
6F698FB090A5F61370A59114FC9F14BE510959A84AB1A5FC12C2332D813E779EEC6C5BBBD82
57996E6D860A7084D5C04A18949645E7DB9DD5F8AE9ACF2D040FBBB463097A01B9D50302C
0436E5B1261469CDF2CCDDDB38E69FE83B61CC8181191DB5F0552EE073A06EA76E2D9918A5
36FC7729FF3E2914F668C793F1D21315205A5649048AA4BC443BB43C5EB367AF431A831A0D8
0D4F4EF2817B2CE25BD81792AA19085B928CC8A2076A4859D568F1B02157DAD57C79AA8283
AB8A969AA2952E06D180DDABBF76F434D86902381052F8CAC71AB998F027BE4042CE51C7F
22A7C507EF6993F31A03BB0918DB9E3FD42CAC5F709C40EE926846387CD228E0351D6AA9D
4AC9D77CC0ABEFA57E4D28991299B1F138ADC6EBB4E2A1DCC20E5CDEAE4BB9433C1F479
5F0B1644167761519378CB5541F9FF8D47E21B200

ID: 363021781

KEY:

3336333032313738315FDAA9F37EDB5A55BA661A87EE387B598A2F160D056E5C36C308B0CE
C9821A82B25FBBE384760678EF9EE47A869DC99BE2045F25ADF36135E1E55B9603A15DCC74
EC20A8C2BA2E703059DCDD4AD087196ADE6D5F06E884595FFE81401663A00C5E9577984627
398889A7D38A1DACBDCA178FBB9AD3AA76E8EE8C045B9480DC1F40CF591B77B390760405F
C959DF245FE1754EED46A53FBCD4189A7D5D8C2CC4A846903CA5C0B612507127A98B187D4
22BE90306D2AA7A13BB9DCCCEB5C947D6B0E7F72C749C73914E3B23A73C22E7870D10B97E
32FDA2F2A76B27B5E8F4BF2DF77385354E33B21DCC1E3CA58D605C7C22A96F1AB79A705A
29A11178CB07A9686012FE9DEB7A6F91D00E153370FB5859D99E8C9B6B9296225181AE49400
9CC47FC6F49157345AE485DFBF4B5E52B6FF9B6FE3B3D480F07D480926EA3EAB7404517997
26DDFF69E18C1DF3E5764C60BEF0BC5361400

?

12321 - May 24, 2017, 1:33 am

there is progress with this problem...

how to fix with hex by Kestukas:

[hxxps://support.emsisoft.com/topic/27231-cry9-invalid-crypton-file-pair/?do=findComment&comment=171003](https://support.emsisoft.com/topic/27231-cry9-invalid-crypton-file-pair/?do=findComment&comment=171003)

how to fix jpeg by matwachich (now it's beta, wait day or 2 for final):

[hxxps://github.com/matwachich/recover_jpeg/](https://github.com/matwachich/recover_jpeg/)

12321 - June 6, 2017, 12:36 am

bad news from emsisoft:Quote:We know everything there is to know about the format and how these keys are created. It is because we know exactly how those keys are generated and used that we know we can't do anything at least for the time being. While an attack is still possible, it simply would take too long to be feasible (we are talking many years here).

Kisame? - June 6, 2017, 12:43 am

(Jun 6, 2017 12:36 AM)12321 Wrote: [\[CITE\]](#) bad news from emsisoft:

You have 2 options now:

1. Reinstall your OS, resulting into the loss of all data.
2. Research the specific ransom, and see if other people got their files back upon payment. If there are important files and the ransom is pay-able, I'd go with this option if it actually would result into your files being restored.

Wish you the best. If you didn't download anything and you recently "resetted" (which I assume means reinstalled) your PC, then it might be some exploit was used (for example, the recent EternalBlue) considering you might have not updated your system after reinstalling, resulting in your system being vulnerable.

In the future, make sure to:

1. Install all windows updates
2. Install an antivirus (I recommend ESET NOD32 + Malwarebytes)
3. Turn on your firewall

Good luck in the future, OP.

5chn4pp - June 6, 2017, 1:15 am

(Jun 6, 2017 12:43 AM)Uchiha Madara Wrote: [\[CITE\]](#) -snip-

Normally if you pay you'll get the key, that is unless you're very unlucky.

Kisame? - June 6, 2017, 1:56 am

(Jun 6, 2017 01:15 AM)Satudarah Wrote: [\[CITE\]](#) Normally if you pay you'll get the key, that is unless you're very unlucky.

That's true, but you'll need to code such a system into your ransom and some people are scumbags and won't even bother doing that much.

12321 - June 7, 2017, 12:47 am

i already reinstalled, but i have ~2000 photos that i want back...

i saw that it's about 70% people got back and 30% didn't... (the one that paid)

also almost all links for onion ransom (cry26) are dead now, scumbags are now sitting in help against ransom forums and sending PMs for payments...

for example this scumbag:Code hxxps://www.bleepingcomputer.com/forums/u/1044806/x3mx3m/

Quote:I can help but for \$ you yourself are looking for difficult ways here then and sit in place no one will help you in vain is wasting your time

Quote:Well, then you already in the black list, though beg, do not get your files back

12321 - June 22, 2017, 2:52 am

i saw in some place that onion's (cry36) encryptor was released...

can anyone confirm?

Aura - June 22, 2017, 4:27 am

Kaspersky got their hands on a couple of keys used by Cry36, so you could try their RakhniDecryptor. Just try it on one file (back up it first) and see if it works or not.

Carbanak - June 23, 2017, 2:53 am

From analysing the tor hidden services related to the ransomware, don't pay because the hidden services are down and most likely the private key has not even been generated to decrypt your files.

12321 - June 25, 2017, 12:41 am

(Jun 22, 2017 04:27 AM)Aur? Wrote: [\[CITE\]](#) Kaspersky got their hands on a couple of keys used by Cry36, so you could try their RakhniDecryptor. Just try it on one file (back up it first) and see if it works or not.kaspersky's answer:Quote:Unfortunately, currently we cannot decrypt files encrypted by this malware variant. If we manage to decrypt them in the future, we will notify you.

Aura - June 26, 2017, 5:47 pm

No there's no free decryption solution for it yet then.

12321 - August 4, 2017, 2:57 am

very bad news: ?

emsisoft:Quote:We classified Cry36 as not feasible to decrypt using the restrictions we try to operate within. Kaspersky was able to "liberate" some of the private keys, so you can try to contact them. But it is highly unlikely that there will be a new decrypter for Cry36 from us.

bleepingcomputer:Quote:Unfortunately, Cry36 is not decryptable at this time. If possible, your best option is to restore from backups.

12321 - August 28, 2017, 6:26 am

EMSISOFT's updateQuote:Avast was looking into Cry36 as well but ultimately came to the same conclusion that we did, that decryption is infeasible

anyone have good news about cry36's cure?

12321 - September 29, 2017, 9:01 am

any news? ?

.....

12321 - November 3, 2017, 11:25 am

any good news?

.....

12321 - December 11, 2017, 2:11 am

any good news?

.....

12321 - January 6, 2018, 3:23 am

almost every teams that was working on cure for cry36 confirmed that they cant decrypt it...

12321 - March 17, 2018, 1:59 am

anyone have some news?

or to delete photos because there is no way to fix them? :(

12321 - September 23, 2018, 12:04 pm

anyone have good news about cry36?

Aura - September 23, 2018, 5:25 pm

I really doubt HF will have any breaking news on malware before websites like BleepingComputer and Emsisoft (at least when it comes to Ransomware). So your best bet is to stick to these as information sources.