

Forum:[Hack Forums](#)

Thread: [CTB-Locker](#)

jozsi777 - January 23, 2015, 7:54 am

Hello.

I've got a virus called CTB-Locker and because of that virus, my files encrypted like, I had a word file called: shoot.doc and it is now shoot.doc.qwhejkqw and also if I open the file after renamed it, then it contains only strings and random characters, I know it's encrypted, can anyone help me? Unfortunately I cannot recover my data to a previous backup point, I did virus scan malwarebytes and rougekill, also with eset nod32 but I need help to recover my files so I can read them again.

Thank you for helping me out.

Here is a link how does it look like:

<http://deletemalware.blogspot.hu/>

realrbn - January 23, 2015, 8:13 am

I don't think you can recover it. You either pay, or reinstall.

-Hyperion - January 23, 2015, 8:50 am

You do not have to reinstall just follow all instructions

<https://hackforums.net/showthread.php?tid=4558828> exactly and post the logs here.

Also read this here

<http://www.bleepingcomputer.com/virus-removal/ctb-locker-ransomware-information#discover> it is possible to get your files restored after removal. Unfortunately if those methods fail your files are gone

SIM-2223238 - January 23, 2015, 9:52 am

What worked for me fine, is adding a new user to your PC, and then remove the old one.

Worked for me tho, not sure If it works for everyone.

-Hyperion - January 23, 2015, 10:15 am

(Jan 23, 2015 10:52 AM)Aggron Wrote: [\[CITE\]](#) What worked for me fine, is adding a new user to your PC, and then remove the old one.

Worked for me tho, not sure If it works for everyone.

That does not recover his files or remove the infection

jozsi777 - January 23, 2015, 12:21 pm

Ok, then it is impossible to recover my files if there was not set to backup (previous version) on my C: it was on so I can recover my files but there were just a few, but on my D:, and F: it was not set so it is impossible now to recover my files? I do think so, what about decrypting somehow the files? Any idea for decrypting elliptical curve I know it's really hard, almost impossible but maybe there will be a solution soon, or maybe the best if I wait a month and hope there will be method to decrypt it.

It is impossible to pay them, I tried yesterday the link under Linux, and it was not possible, there was an 500 error, and saying it's not working, anyway I won't pay these criminals, hoping to have some solution...

-Hyperion - January 23, 2015, 12:25 pm

Did you read the instructions I posted? Everything is explained

jozsi777 - January 23, 2015, 12:30 pm

thanks, I've already saw that shadow explorer not working, I haven't set the previous data protection, so I cannot recover my files I think it is not possible, or if it then how?

Thanks

I dont think im infected, but will try all the instruction that you wrote down, but anyway if there will be some viruses, or malwares, and clean them, my files wont change the encryption so they stay infected.

-Hyperion - January 23, 2015, 12:33 pm

It's not possible the key used to encrypt them expires

jozsi777 - January 23, 2015, 12:41 pm

Thanks for helping, I know that its impossible but I wanted to be sure, that its impossible, to recover, I hope there will be a solution in a month. Thanks for helping again.

woahxx - January 24, 2015, 12:40 pm

It's impossible to recover as soon you are encrypted. Pay or reinstall.