

Forum:[Hack Forums](#)

Thread: [CryptoLocker 3.0](#)

Phil - March 28, 2015, 2:52 am

Hey guys,

So my dad's company has been Crypto'd (it has many important files related to the business) and I was wondering if there is any way to get it back? I did my own research, tried programs and websites but nothing seems to work.

Any of you have an idea of how I could get it back? I even tried System Restore, but it is still there.

Thanks.

obviouslyracist - March 28, 2015, 2:55 am

CryptoLocker 3.0 doesn't have a fix.

The only way to get the files is to pay the ransom.

Sorry. :(

Phil - March 28, 2015, 2:56 am

(Mar 28, 2015 02:55 AM)obviouslyracist Wrote: [\[CITE\]](#) CryptoLocker 3.0 doesn't have a fix.

The only way to get the files is to pay the ransom.

Sorry. :(

Damn that is a pain. I wish someone did make a fix for it ?

5chn4pp - March 28, 2015, 4:11 am

have you tried going into safemode and do something there?

archangel.dmitry - March 28, 2015, 7:51 am

(Mar 28, 2015 04:11 AM)One Virus(° ? °) Wrote: [\[CITE\]](#) have you tried going into safemode and do something there?

If it is CryptoLocker 3.0, safe mode is useless. The only way to fight CL 3.0 is to have backups.

5chn4pp - March 28, 2015, 8:04 am

(Mar 28, 2015 07:51 AM)archangel.dmitry Wrote: [\[CITE\]](#) If it is CryptoLocker 3.0, safe mode is useless. The only way to fight CL 3.0 is to have backups.

ok, thats good to know, how spread is it?

Phil - March 28, 2015, 11:27 am

(Mar 28, 2015 08:04 AM)One Virus(° ? °) Wrote: [\[CITE\]](#) ok, thats good to know, how spread is it?

Pretty spread, 603 files encrypted ?

5chn4pp - March 28, 2015, 11:32 am

(Mar 28, 2015 11:27 AM)DehPhil Wrote: [\[CITE\]](#) Pretty spread, 603 files encrypted ?

oh, i meant how many computers had it? also, 600 files is nothing.

Anti-Malware - March 28, 2015, 11:34 am

- 1) If your computer has been infected by CryptoLocker, disconnect from your wireless or wired network right away to prevent further file encryption.
- 2) Decide if you want to pay the ransom and have files decrypted or try to restore the files yourself.
- 3) If you choose to pay the ransom, do it BEFORE removing the virus. Once the ransom is paid, your files will all become decrypted over the course of 3-4 days.

Davy - March 28, 2015, 11:59 am

Dang, it sucks for you man, but I have to admit, thats pretty original.

Phil - March 28, 2015, 2:34 pm

(Mar 28, 2015 11:32 AM)One Virus(° ? °) Wrote: [\[CITE\]](#) oh, i meant how many computers had it? also, 600 files is nothing.

Yeah 600 files is nothing but its the files I require most.

Knautschtabak - April 1, 2015, 12:19 pm

You can try to recover files from shadow copies. But that's pretty much it.

See:

Quote:To restore the previous version of a file using the traditional Windows interface, just right-click the file in question and choose Properties. If System Restore is enabled or your administrator has enabled Shadow Copies through Group Policy, you should be able to see the Previous Versions tab in the Properties window. This will list all of the versions on record of the file. Choose a version before the Cryptolocker infection and then click either Copy to export a copy of the file somewhere else, or Restore to pop the backup right where the encrypted file belongs. You can open the files directly from this box too if you are not sure of the exact date and time of infection.

Quote:1) If your computer has been infected by CryptoLocker, disconnect from your wireless or wired network right away to prevent further file encryption.

Cryptolocker does not need the internet to encrypt files. So why should this prevent encryption?

Pharmacist - April 1, 2015, 12:21 pm

(Apr 1, 2015 12:19 PM)Knautschtabak Wrote: [\[CITE\]](#) You can try to recover files from shadow copies. But that's pretty much it.

See:

Cryptolocker does not need the internet to encrypt files. So why should this prevent encryption?
CL deletes shadow copies.

Its really an amazing work of art, if only they had used that skill for something other than this..

Knautschtabak - April 1, 2015, 12:45 pm

(Apr 1, 2015 12:21 PM)Humiliated Wrote: [\[CITE\]](#) CL deletes shadow copies.

Its really an amazing work of art, if only they had used that skill for something other than this..

Woah, so they thought of everything.

Pharmacist - April 1, 2015, 1:00 pm

(Apr 1, 2015 12:45 PM)Knautschtabak Wrote: [\[CITE\]](#) Woah, so they thought of everything.

Yup.

I've never actually seen this 3.0 version.

But it doesn't seem that it would be extremely hard to create, mostly, all they had to do is know the basics of cryptography, and execute cmd commands. And that's it!

SIM-2096295 - April 1, 2015, 4:10 pm

google found this video, no idea if CryptoWall 3.0 is the same thing or if this works but maybe it will help <https://www.youtube.com/watch?v=gPelrlpQIJg>

Herbert - April 2, 2015, 6:28 am

[Video: <https://www.youtube.com/watch?v=gPelrlpQIJg>]

Ghanem - April 2, 2015, 8:57 am

(Apr 2, 2015 06:28 AM)John Herbert Wrote: [\[CITE\]](#) [Video: <https://www.youtube.com/watch?v=gPelrlpQIJg>]

Everyone can remove it, even without guide.

People want to decrypt their files, not to remove the virus.

Herbert - April 2, 2015, 9:44 am

(Apr 2, 2015 08:57 AM)Ghanem Wrote: [\[CITE\]](#) Everyone can remove it, even without guide.

People want to decrypt their files, not to remove the virus.

hmm, how about a system restore point?

just keep loading up restore points till you got your files back without the virus.

Ghanem - April 2, 2015, 10:27 am

(Apr 2, 2015 09:44 AM)John Herbert Wrote: [\[CITE\]](#) hmm, how about a system restore point?

just keep loading up restore points till you got your files back without the virus.

'heard system restore themselves doesn't remove the encryption.

Shadow Copies might work by CryptoLocker removes them.

Pharmacist - April 2, 2015, 11:58 am

(Apr 2, 2015 09:44 AM)John Herbert Wrote: [\[CITE\]](#) hmm, how about a system restore point?

just keep loading up restore points till you got your files back without the virus.

Disables, and deletes all past system restore data.

Along with any other way of recovering it.

The only real way is to pay up, or hope something else works.

(Apr 2, 2015 09:44 AM)John Herbert Wrote: [\[CITE\]](#) hmm, how about a system restore point?

just keep loading up restore points till you got your files back without the virus.

Disables, and deletes all past system restore data.

Along with any other way of recovering it.

The only real way is to pay up, or hope something else works.

-Hyperion - April 2, 2015, 3:36 pm

(Apr 2, 2015 09:44 AM)John Herbert Wrote: [\[CITE\]](#) hmm, how about a system restore point?

just keep loading up restore points till you got your files back without the virus.

crypto disables and removes them there is currently no a single way to get the files back with version 3

Herbert - April 2, 2015, 5:07 pm

well, some say it may still work on certain files on 3.0 try Kaspersky's RectorDecryptor.exe or Kaspersky's RakhniDecryptor.exe these aren't made for this particular ransomware if it doesn't work best guess is to wait for one to come out.

Converts Bitcoins2015 - *May 16, 2015, 10:17 am*

(Mar 28, 2015 02:55 AM)obviouslyracist Wrote: [\[CITE\]](#) CryptoLocker 3.0 doesn't have a fix.

The only way to get the files is to pay the ransom.

Sorry. :(

1 way pay operators ;)

i think