

Forum:[Hack Forums](#)

Thread: [CTB locker crypted pendrive file](#)

Briesanji - December 24, 2015, 5:22 am

Hello guys

My client's computer was infected with CTB-Locker
Unfortunately after he inserted the pendrive a message pop up saying that all files are encrypted and to decrypt it he needs to pay 120\$.

Ok now my clients told me that he doesn't mind about computer files but he absolutely needs the PENDRIVE'S data.

Is there a way to do recover them ?

Knautschtabak - December 24, 2015, 6:57 am

Your only bet is file recovery software, which will only work if you are lucky. With CTBLocker there is no chance to get the files back other than paying the ransom and thus the criminals to continue with their attacks.

LividandGifted - December 24, 2015, 8:00 am

Unfortunately this type of infection usually comes with a 2048 bit RSA encryption (same as Cryptowall) and even with all the computers in the world combined, it would take centuries to decrypt.

With ransomware infections on a Windows OS, you can sometimes clean the infection first, then use a system restore point to go back to a point in time where your files were not encrypted. Shadow Explorer is useful for this. This is not the case with newer ransomware though; they caught on to that and now the infection will usually delete all your system restore points.

You could always format and try to restore with something like R-Studio. Don't even bother with Piriform's Recuva, it's crap. It may find some files to recover, but more often than not, the files are unreadable. This is not the case with R-Studio, it does a fantastic job.

I service a company and they got infected with cryptowall 4.0 - there were no restore points for us to use. The company decided to pay the ransom and they got their files back.

Good luck with whatever approach you decide to take.

Briesanji - December 24, 2015, 3:43 pm

Thanks for all the answers.. ??