How to use ZCB to recover from Cryptolocker and other ransomware

Information

Recently, a virus called **Cryptolocker** has been taking the internet by storm. It is incredibly efficient at what it does: holding files hostage and demanding a ransom to get them back.

There is no guarantee that paying the ransom will unlock the files. Cryptolocker, its variants, and other ransomware are completely illegitimate.

It does so by encrypting your files. Encrypted files cannot be accessed until they are decrypted. Only Cryptolocker has access to the keys required to decrypt the files it encrypts.

However, Cryptolocker (and other, similar ransomware) can be easily defeated with ZCB. Simply restore the files from a backup taken *before* the system was infected.

About Cryptolocker

The idea of a ransom is not new. People have demanded a ransom for hostages–human or otherwise–since time immemorial.

In this digital age, the idea has been extended to the files on your computers, servers, and gadgets. Cryptolocker is, to date, one of the most efficient piece of ransomware ever made. It's simple and devious.

The original version of Cryptolocker does the following:

1. Silently infects your machine(s).
2. Begins encrypting your files, including those on network shares.
3. Displays a notification demanding money to decrypt your files. This demand only appears *after* encryption is complete.
4. Places a time limit on how long you have to pay.
5. Deletes itself, but does not decrypt your files, if you do not pay.

The original Cryptolocker targets Office documents, pictures, and other files that are typically associated with *content* and not necessarily those required to run various programs and applications. For example, infected users can still load Microsoft Word, but they cannot open their Word documents.

No antivirus product (or any *other* product, for that matter) will be able to decrypt your files once they are encrypted.

Once your files are encrypted, your options are very limited. The encrypted files cannot be decrypted without Cryptolocker. Re-infecting yourself doesn't give you a new timer. If you don't pay, your files are permanently locked.

In most cases, only two options are available: restore unencrypted files from a backup, or lose the files forever.

Restore with ZCB!

Restoring older versions of files is simple with Zmanda Cloud Backup! ZCB will try to restore from local backups first, and will fall back to the cloud if those are unavailable.

Most Cryptolocker variants do not target the types of files that ZCB creates for backup, but even if your local backups are damaged, your cloud backups are safe and sound!

1. Visit the Restore page
2. Select a **Restore Point** from a date and time from **before** you were infected.
3. By default, all files will be selected for restore.
    a. Use the **Restore Select** to restore some files.
    b. Use the **Search** option to restore a single file or folder.
4. Review your restore settings. Here you can choose where the files will be restored, what will happen if the file already exists, and more.
5. Click Restore, and confirm your choices when asked to do so.

Once the restore has been started, simply sit back and wait. ZCB will restore your files, unencrypted, just as they were, **before** you were infected! You can be back up and running in a short time, without paying a ransom, and with minimal interruption.