Forum:Hack Forums

Thread: CTB Locker

BLCKBRD - *March 31, 2016, 7:38 am*
Long story short: my dad got infected with CTB Locker. Is there a way to recover the PC and remove this virus?

-DD

Spacefiller - *March 31, 2016, 11:14 am*
I don't think currently there's any way to decrypt files from that ransomware.
Sorry. You could remove it with malwarebytes. Unless it stops you from doing that, if it does, post back here.

BLCKBRD - *March 31, 2016, 11:15 am*
(Mar 31, 2016 11:14 AM)rocket4wheel Wrote: *[CITE]* I don't think currently there's any way to decrypt files from that ransomware.
Sorry. You could remove it with malwarebytes. Unless it stops you from doing that, if it does, post back here.
So the files are all gone?

Spacefiller - *March 31, 2016, 1:19 pm*
There may never be a decryption tool, so assume that they are all gone. :/
Might as well just remove it. Sorry.

spyglass - *March 31, 2016, 3:07 pm*
Op maybe not because there is ways to restore and recover depending on four factors.

The first and main one is to use is a full system back up if you have it.

The Second way is try to use windows previous versions on folders and files.

The third one is to try to use file recovery software.
You could try some trusted ones listed below for this...
R-Undelete Home http://www.r-tt.com
Recuva http://www.piriform.com/recuva
PhotoRec http://www.cgsecurity.org/wiki/PhotoRec
Puran File Recovery http://www.puransoftware.com/File-Recovery.html
Undelete 360 http://www.undelete360.com
Pandora Recovery http://www.pandorarecovery.com
Restoration http://www3.telus.net/mikebike/RESTORATION.html

The fourth way is try to restore with the use of shadow files if possible.
Shadow Explorer http://www.shadowexplorer.com/
There is quite a few reports of the locker and problems with the removal of shadow files with Vssadmin silent so you might get lucky here.

If you go to %MyDocuments%\<random>.html or %C:\Users\All Users\<random>.html you should be able to see every file encrypted.

It is best to try to recover files before you remove the infection.
Sadly the private key is removed from the infected system after infection depending on the version.

Spacefiller - *March 31, 2016, 5:59 pm*

(Mar 31, 2016 03:07 PM)spyglass Wrote: [CITE] The first and main one is to use is a full system back up if you have it.

The Second way is try to use windows previous versions on folders and files.

The third one is to try to use file recovery software.

The fourth way is try to restore with the use of shadow files if possible.
Shadow Explorer
If he has a backup. Backups are only useful if you have really important information such as bitcoin keys. From what I can tell your dad doesnt need or have a backup.

Windows previous versions are disabled by default

File recovery software fixes deleted files. These are encrypted (overwritten with the encrypted version)

idk what shadow explorer is, Im gonna take a look at that

edit: holy shit thanks shadow copy just saved a really important .ino file i had! holy shit thanks shadow copy may work for you OP