

Forum:[Hack Forums](#)

Thread: [Infected with CTB-Locker !! \(Documents Encrypted\)](#)

Im Cold - July 21, 2016, 7:59 pm

Yoo HF Famm

So my dads wife (my step mom) gave me her friends laptop thats infected with a CTB-Locker virus, I did some research and it looks like this bitch is hard to remove... Says you gotta pay a ransom or some shit.. Idk.. But it says if the user tries to use malware removal software it will delete the decryption password.. What can I do?!

Shadow Reign - July 21, 2016, 8:37 pm

(Jul 21, 2016 07:59 PM)bL Nugs Wrote: [\[CITE\]](#) Yoo HF Famm

So my dads wife (my step mom) gave me her friends laptop thats infected with a CTB-Locker virus, I did some research and it looks like this bitch is hard to remove... Says you gotta pay a ransom or some shit.. Idk.. But it says if the user tries to use malware removal software it will delete the decryption password.. What can I do?!

Well i'm not much of a white hatter but I have had issues with ransomware in the past however I removed it manually.

For now, make sure all wireless communication on the infected device is turned off (double or triple check) and begin going through the "services" tab in msconfig or taskmanager. Eventually you'll find a service you may not recognize. Disable that service from startup and check all startup folders for any files connected to this service. if you're unsure, you can always google the service name.

Chances are there are more than one infected area in the system in case the user does just this. So look for any suspicious files in various places such as the hidden folders in the C: drive like ProgramData.

Once you're sure the malware is now unable to start during a bootup, you can now restart the system. Once it has restarted, check the services tab once more to ensure the suspected service is no longer running.

You can now check online for various methods to decrypt the files. Microsoft offers various decrypting services for users who have been infected, although not all decryption services can decrypt the files. You may have to wait until a new decryption service is available.

keep in mind the malware is still on your system but can not run. make sure to download an anti malware service once these steps are complete to fully remove the infection.

However, as long as the ransomware is no longer running, it cannot delete the files.

Keep in mind this is what I did and it worked fine for me, however the ransomware I was infected with wasn't very complex.

I would only suggest you do this method if you know what you're doing and you cannot find any

help anywhere else.

I would also suggest you wait at least a full 24 hours before trying anything yourself to give the White Hat team on this forum a chance to compile their responses. All too often I see people who lack patience and attempt things themselves without knowing what they're doing and end up breaking something.

Woods - July 21, 2016, 8:43 pm

I honestly am paying no money to have access to my computer, I will manually wipe my computer down and reinstall the OS before I give some fucker some money.

Dem?n - July 22, 2016, 8:29 am

(Jul 21, 2016 08:43 PM)The Owl Wrote: [\[CITE\]](#) I honestly am paying no money to have access to my computer, I will manually wipe my computer down and reinstall the OS before I give some fucker some money.

The encryption only affects documents of the machine, not executables or any of the like. You'd be safe using it, just throw a good AV onto it like ESET. You can also format. It doesn't matter.

Im Cold - July 22, 2016, 10:00 am

(Jul 21, 2016 08:37 PM)Shadow Reign Wrote: [\[CITE\]](#) Well i'm not much of a white hatter but I have had issues with ransomware in the past however I removed it manually.

For now, make sure all wireless communication on the infected device is turned off (double or triple check) and begin going through the "services" tab in msconfig or taskmanager. Eventually you'll find a service you may not recognize. Disable that service from startup and check all startup folders for any files connected to this service. if you're unsure, you can always google the service name.

Chances are there are more than one infected area in the system in case the user does just this. So look for any suspicious files in various places such as the hidden folders in the C: drive like ProgramData.

Once you're sure the malware is now unable to start during a bootup, you can now restart the system. Once it has restarted, check the services tab once more to ensure the suspected service is no longer running.

You can now check online for various methods to decrypt the files. Microsoft offers various decrypting services for users who have been infected, although not all decryption services can decrypt the files. You may have to wait until a new decryption service is available.

keep in mind the malware is still on your system but can not run. make sure to download an anti malware service once these steps are complete to fully remove the infection.

However, as long as the ransomware is no longer running, it cannot delete the files.

Keep in mind this is what I did and it worked fine for me, however the ransomware I was infected with wasn't very complex.

I would only suggest you do this method if you know what you're doing and you cannot find any help anywhere else.

I would also suggest you wait at least a full 24 hours before trying anything yourself to give the

White Hat team on this forum a chance to compile their responses. All too often I see people who lack patience and attempt things themselves without knowing what they're doing and end up breaking something.

Could anyone possibly help me over TeamViewer with this? Shit is complicated as fuck. I tried several programs to remove it as well.. a few threats found but nothing what you said..

LogoiLab - July 22, 2016, 10:10 am

I'm assuming its windows cause ransomware is rare for Linux...and a little less common for mac... If the documents that it encrypted aren't needed just go to the pc settings and restore it to factory default(be sure to tell it to delete all programs) this only works for windows 8.1 and 10 so for 7 and below you'll have to reinstall. If the files are necessary to be recovered you're either out of luck, have to pay, or you can do a deep forensic analysis which takes time and practice and you can attempt to find the C2 server and trick it into giving you the private key for the encrypted files.

Long Morrison - July 22, 2016, 10:11 am

Have you tried using google?
did you do system restore

Spacefiller - July 22, 2016, 10:25 am

Your documents are encrypted. I may have a method to retrieve your files. This is untested, but if you give me permission, may I try it? Add me on skype, sent you a PM

SlavedWizard - July 25, 2016, 1:22 pm

"How to Decrypt files infected with CTB Locker

There is only one known way to remove this virus successfully – reversing your files to a time when they were not infected. "

source: fufufu how to remove dot guide slash ctb-locker-decrypt-and-removal slash

Wish u best.

Shadow Reign - July 25, 2016, 10:00 pm

<https://www.nomoreransom.org/decryption-tools.html>

You can try this out as well.