

Forum:[Hack Forums](#)

Thread: [Remove ransomware/cryptolocker](#)

xeonx - May 24, 2015, 3:34 pm

How would you go through on removing this? I've never seen this specific version before.

note: I am not infected I'm asking on behalf of a friend.

Niko - May 24, 2015, 3:46 pm

First things first, Are they able to open any files? If they can, it may just be scareware.

If the files are encrypted, since that is 0.1Btc, I would pay it. Thats only about \$25. However, if it is paid, there may be the chance of it being a scam. But it being only \$25 for all of ones files, It isn't that bad of an idea.

Diddle - May 24, 2015, 6:08 pm

can you open any thing? if not reinstall the OS some files lost but atleast you can restart

Ta-kun - May 24, 2015, 6:11 pm

Is what he has on that PC of any real value? If not then I'd just format the hard drive and then start out fresh. I'm sure they could use it anyways.

crazyycast13 - May 24, 2015, 6:38 pm

Hello I hail from the cryptography section.

I can tell you right now you are most likely royally screwed. If you haven't yet, check online to see if that is one of the poorly coded cryptolockers which store the encryption key on the victim PC.

EDIT: it's only .1 BTC, that's pretty cheap, I would try paying to get your files back if they are worth 25usd to you.

lavish - May 24, 2015, 9:57 pm

(May 24, 2015 06:38 PM)crazyycast13 Wrote: [\[CITE\]](#) Hello I hail from the cryptography section.

I can tell you right now you are most likely royally screwed. If you haven't yet, check online to see if that is one of the poorly coded cryptolockers which store the encryption key on the victim PC.

EDIT: it's only .1 BTC, that's pretty cheap, I would try paying to get your files back if they are worth 25usd to you.I cry'd when I saw your signature hahaha.

OT: try using ShadowExplorer to look for shadow copies.

cyberducky - May 24, 2015, 10:26 pm

Does your friend have a previous restore point?

ProtectNull™ - May 24, 2015, 10:29 pm

Lmao, hes asking for help. I don't think OP wants to pay 0.1 If I were you OP, let someone professionally here, help you with that.

crazyycast13 - May 24, 2015, 10:35 pm

(May 24, 2015 10:29 PM)Matthewbmx™ Wrote: [\[CITE\]](#) Lmao, hes asking for help. I don't think OP wants to pay 0.1 If I were you OP, let someone professionally here, help you with that.

I am currently working on anticryptoware software. I can safely tell you following my post is the right way of doing things, and trying to remove the virus without paying is the worst way of going about it if your files are worth more than 25 dollars.

cyberducky - May 24, 2015, 10:39 pm

(May 24, 2015 10:35 PM)crazyycast13 Wrote: [\[CITE\]](#) I am currently working on anticryptoware software. I can safely tell you following my post is the right way of doing things, and trying to remove the virus without paying is the worst way of going about it if your files are worth more than 25 dollars.

You are wrong. OP DO NOT under any circumstances pay the ransom. There is not a single confirmed case of people getting their files back after paying the ransom.

I can assist you in getting your files back. It is possible to get your files back.

Knautschtabak - May 25, 2015, 10:44 am

Please read through the points below to ensure this process moves as quickly and efficiently as possible. Ensure you read through my instructions thoroughly, and carry out each step in the order specified.

Please do not run any tools or take any steps other than those I provide for you. Independent efforts may make matters worse, and will affect my ability in providing the best set of instructions for you.

Please backup important files before proceeding with my instructions. Malware removal can be unpredictable at times.

If you come across any issues whilst following my instructions, please stop and inform me of the issue in as much detail as possible. Please do not hesitate to ask before proceeding.

I will notify you when I believe your computer is free of malware. Please bear in mind, absence of symptoms does not necessarily correlate to absence of malware, so please wait until the "All Clean".

Step 1: Farbar Recovery Scan Tool (FRST) ScanPlease download [Farbar Recovery Scan Tool \(x32\)](#) or [Farbar Recovery Scan Tool \(x64\)](#) and save the file to your Desktop.

Note: Download and run the version compatible with your system (32 or 64-bit). Download both if you're unsure; only one will run.

Right-Click FRST.exe or FRST64.exe and select Run as Administrator

Click Yes to the disclaimer.

Ensure the Addition.txt box is checked.

Click the Scan button and let the program run.

Upon completion, click OK, then OK on the Addition.txt pop up screen.

Two logs (FRST.txt & Addition.txt) will now be open on your Desktop. Copy the contents of both logs and paste them to pastebin.com. Post the link here.

Step 2: RogueKillerDownload [RogueKiller \(32 bit\)](#)/[RogueKiller \(64 bit\)](#) and save the file to your Desktop.

Note: Download and run the version compatible with your system (32 or 64-bit). Download the first (32-bit) if you're unsure.

Close any running programs.

Right-Click RogueKiller.exe and select Run as administrator to run the program.

Allow the Prescan to complete. Upon completion, a window will open. Click Accept.

A browser window may open. Close the browser window.

Click . Upon completion, click .

Close the program. Do not fix anything!

A log (RKreport.txt) will be open. Copy the contents of the log to pastebin.com, click Submit and paste the link to it in your next reply.

xeonx - May 25, 2015, 10:53 am

(May 25, 2015 10:44 AM)Knautschtabak Wrote: [\[CITE\]](#) Please read through the points below to ensure this process moves as quickly and efficiently as possible. Ensure you read through my instructions thoroughly, and carry out each step in the order specified.

Please do not run any tools or take any steps other than those I provide for you. Independent efforts may make matters worse, and will affect my ability in providing the best set of instructions for you.

Please backup important files before proceeding with my instructions. Malware removal can be unpredictable at times.

If you come across any issues whilst following my instructions, please stop and inform me of the issue in as much detail as possible. Please do not hesitate to ask before proceeding.

I will notify you when I believe your computer is free of malware. Please bear in mind, absence of symptoms does not necessarily correlate to absence of malware, so please wait until the "All Clean".

Step 1: Farbar Recovery Scan Tool (FRST) ScanPlease download [Farbar Recovery Scan Tool \(x32\)](#) or [Farbar Recovery Scan Tool \(x64\)](#) and save the file to your Desktop.

Note: Download and run the version compatible with your system (32 or 64-bit). Download both if you're unsure; only one will run.

Right-Click FRST.exe or FRST64.exe and select Run as Administrator

Click Yes to the disclaimer.

Ensure the Addition.txt box is checked.

Click the Scan button and let the program run.

Upon completion, click OK, then OK on the Addition.txt pop up screen.

Two logs (FRST.txt & Addition.txt) will now be open on your Desktop. Copy the contents of both logs and paste them to pastebin.com. Post the link here.

Step 2: RogueKillerDownload [RogueKiller \(32 bit\)](#)/[RogueKiller \(64 bit\)](#) and save the file to your Desktop.

Note: Download and run the version compatible with your system (32 or 64-bit). Download the first (32-bit) if you're unsure.

Close any running programs.

Right-Click RogueKiller.exe and select Run as administrator to run the program.

Allow the Prescan to complete. Upon completion, a window will open. Click Accept.

A browser window may open. Close the browser window.

Click . Upon completion, click .

Close the program. Do not fix anything!

A log (RKreport.txt) will be open. Copy the contents of the log to pastebin.com, click Submit and paste the link to it in your next reply.

isnt that copy paster 100% from tha sneak? anyways I solved the problem by decrypting the files using the key.dat thanks for suggestions :)