EXIGENT

DRIVEN BY EXCELLENCE

The Guide to CryptoLocker Prevention and Removal

An introduction to CryptoLocker: The basics

CryptoLocker is a type of malicious software (malware) that makes data on your computer (documents, pictures, music and so on) unreadable by encrypting it using RSA-2048 bit keys; it then demands payment to un-encrypt them. Once you pay (to the tune of several hundred USD via prepaid voucher or virtual currency known as Bitcoin), you get your files back. The malware even puts a deadline on how long you have to pay the ransom. CryptoLocker affects Windows computers and usually finds its way onto them via email attachments.

Is Your Cloud Data Secure?

The fact that you are backing up data to the cloud is a good thing – but it's not the act of backing up that's the issue. The problem with typical cloud backup implementations is that they're set to synchronize; your backed-up data in the cloud is maintained as a mirror copy of what's currently on your computer. Ordinarily that's ideal – unless those files are encrypted by CryptoLocker, in which case they'll be synchronized to the cloud by your backup software. Later in this document we'll look at how you can ensure your backup doesn't get corrupted.

Cloud-to-cloud backup solutions offer an additional secure copy of your data that maintains prior versions – bingo, the un-encrypted files without the CryptoLocker infection.

Removing the CryptoLocker malware

What if it's too late and you've already been infected? If your files have been encrypted you're unfortunately out of luck. The files are encrypted in such a way that it's all but impossible to decrypt them (unless you pay the ransom, in which case you'd [likely] regain access to your files).

To remove the CryptoLocker malware we're going to use software called Malwarebytes; the free version will detect and remove the malware.

The malware even puts a deadline on how long you have to pay the ransom. CryptoLocker affects Windows computers and usually finds its way onto them via email attachments.

Download Malwarebytes here: **http://www.malwarebytes.org/**

Do the following once you have Malwarebytes installed:

- Run a Quick Scan.
- Click **Show Results** once the scan completes.
- If CryptoLocker is on your computer, you'll see entries on this page for **Trojan.Ransom**. Make sure all of them are checked and click **Remove Selected**.
- Restart your computer to finish the process.
- Again, note that this process is effective at removing the CryptoLocker malware itself, not the encryption of your files.

CryptoLocker malware prevention tips

We provided step-by-step instructions on how to remove CryptoLocker if you've already been affected but prevention is key. Here are eight tips to stay safe. **Follow these tips:**

- Install a reputable anti-virus software that has on-demand scanning.
- Schedule your anti-virus software to automatically run scans at least once per week.
- Always double-check the sender of any emails you receive and if you don't know the sender, proceed with caution.
- Never click on email attachments unless you know exactly what the attachment is.
- Don't click on links within emails unless you know where the link is going.
- Keep a separate backup of your personal files away from your computer.
- Set up and stick to a regular backup schedule.
- If you use cloud backup services, consider investing in a cloud-to-cloud secure backup solution as a plan.

Keep your backups safe with cloud-to-cloud backup

In the prevention tips above, we suggest making a backup of your backup via cloud-to-cloud backup. Cloud-to-cloud backup solutions offer an additional secure copy of your data that maintains prior versions – bingo, the un-encrypted files without the CryptoLocker infection. These versioned files are inaccessible and unchangeable by CryptoLocker. They also insure against one of the leading causes of data loss, accidental deletion, by keeping any deleted files even if you were to remove them from your computer.

Conclusion

The CryptoLocker virus and related cryptovirus variants can devastate your business. We hope these tips are helpful in planning for, or containing, a CryptoLocker infection. Keep in mind that this malware is modified regularly to bypass your anti-virus software, so we recommend training all employees to act quickly and disconnect from the network, or turn off their computers, if they suspect they have been infected. This training can help prevent the spread of the virus and contain the damage.

Quick-response training is especially important since mobile employees may be infected off-site, and can bring the virus back to the network. This enables the virus to bypass your firewall and infect your network when your employee returns to the office. In addition to these steps, we also recommend that you review and adjust your backup and data retention plans to ensure that you have the ability to restore your data if your network becomes infected.

To combat these potentially destructive viruses, we are offering a **FREE virus prevention and data recovery analysis** (a value of up to $2,500). We will review the following components and make recommendations for any corrective actions:

1. **The current state of your network and overall IT security including:**
    - **a.** Your backup and disaster recovery strategy
    - **b.** Your anti-virus mechanisms
    - **c.** Your current firewall and its capabilities
    - **d.** What you might be missing that is leaving you vulnerable to attack and data loss

The analysis is FREE, confidential and without obligation, but the information learned from it can be priceless. Contact us at **877.EXIGENT** (877.394.4368) or sign-up online for a **FREE virus prevention and data recover analysis** to see how we can help you build a digital fortress around your precious data.