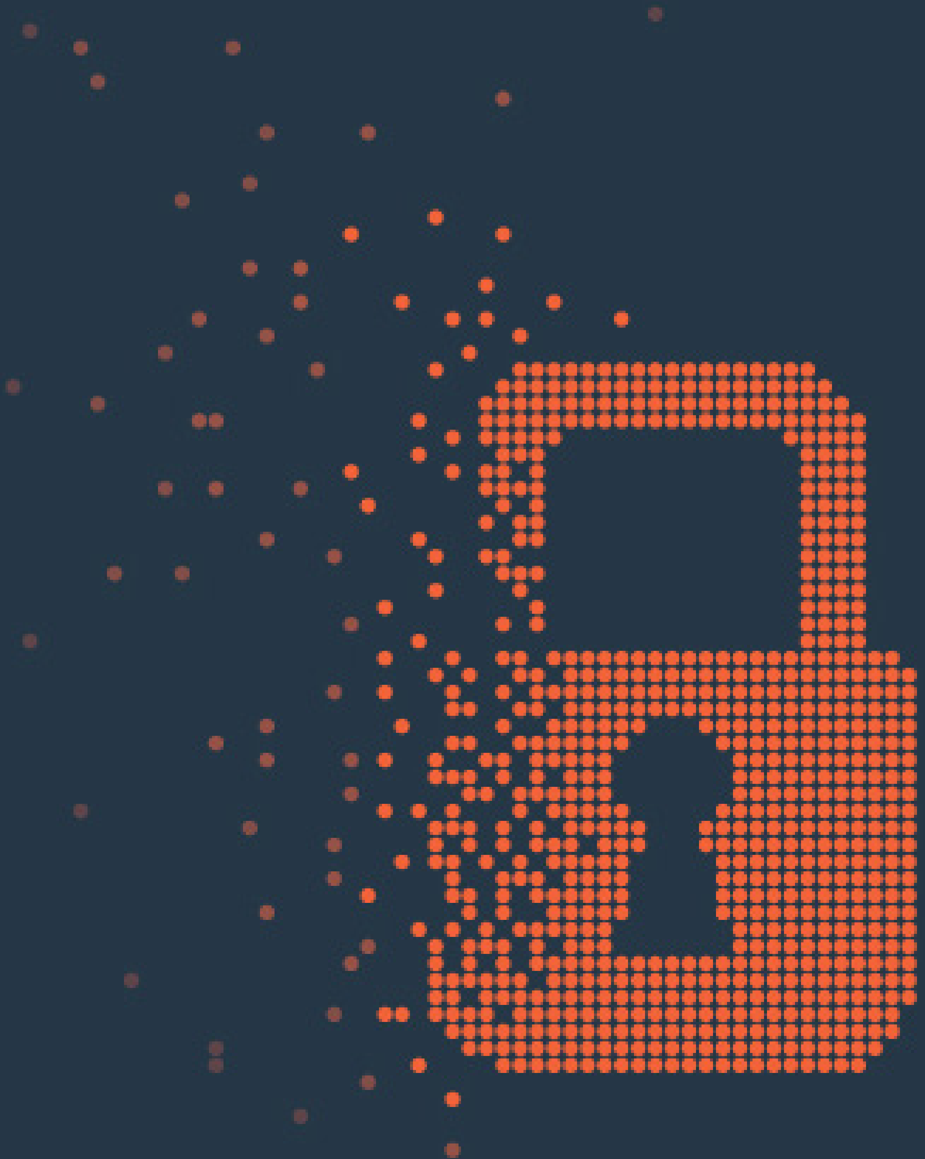
datto

The Guide to CryptoLocker Prevention and Removal

By Charles P. Jefferies



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 attachment.

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. Your backup isn't what you thought it was, just like that. 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 [like] 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.

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 for the vast majority, prevention is key. Here are eight tips to stay safe.

Follow the following 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 unencrypted 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.

Cloud-to-cloud backup is a worthwhile preventative solution; it's a backup for your backup in other words. It backs up data you store in Google Drive for instance and not only creates an additional secure copy but stores previous versions. In CryptoLocker terms, that means you would have the unencrypted versions. And of course with the second copy, it has the added benefit of preventing data loss via accidental deletion.

Conclusion

The morale of the story is that while the CryptoLocker malware itself can be removed easily enough via Malwarebytes free edition, prevention is crucial. Install appropriate anti-virus software, be wary of any emails that are sent to you from unknown senders and have appropriate backup in place – whether it's a physical copy or a cloud-to-cloud backup solution.

About Datto

Datto is an innovative provider of comprehensive backup, recovery, and business continuity solutions used by thousands of managed service providers worldwide. Datto's 180+ PB purpose-built cloud and family of software and hardware devices provide Total Data Protection everywhere business data lives. Whether business data is on-prem in a physical or virtual server, in the cloud, or in SaaS applications, only Datto offers end-to-end recoverability and single-vendor accountability. Learn more at www.datto.com.

Corporate Headquarters
Datto, Inc.
101 Merritt 7, Norwalk, CT 06851
United States
partners@datto.com • www.datto.com
888.294.6312

Regional Offices

Norwalk, CT	888.294.6312
Boston, MA	800.571.4984
Toronto, CAN	877.811.0577
Reading, UK	+44 (0) 118 402 9606

3/9/16