CRYPTO LOCKER VIRUS

My computer got the virus, fortunately we did a back up to a separate disk
once a month as the virus got into the back up that runs in the
background. I believe it came through a phone update to Mozilla Firefox,
So just warning everyone to back up to a separate disk and be carefull.

What is a phone update of Mozilla Firefox? and how do you protect yourself with only a once-a-month backup? I don't understand that whole message, including getting the virus on your computer via the backup.

Miriam N. Jacobson, Pennsylvania

We've seen several incidents of CryptoLocker (and it's variants and copycats). They almost always come through infected email attachments in our experience.

Disclaimer: CryptoLocker is a nasty mess. I've never been a lawyer.

Ben M. Schorr, Arizona

Cryptolocker and its variants are nasty. If your backup system backs your system up continuously and contemporaneously with the changes you make on your system, then as the system backs up the virus spreads to the backup and potentially even to the prior backups stored on the backup system. By the time you realize you are infected there's nothing to backup from because all of the backups are infected, too. The idea behind the once-a-month separate disk backup is to have a backup which is done infrequently enough so that if you realize you are dealing with Cryptolocker (or another virus) and it has already spread to and locked down your primary backup system, you can turn to the once-a-month separate disk backup (which was hopefully last updated prior to the inception of the infection and so is unaffected). Losing a month is not pleasant, but it is better than losing everything. My primary backup is done via CrashPlan, automatically and continuously, but I also do a separate manual once-a-week backup to an external Passport drive that I only connect to my PC during the backup process.

Daniel Alan Terner, Florida

Daniel, I also have cloud Carbonite continuous backups of my data files, I do daily backups to a set of external disks of data files, and weekly backups of the full system, also to Passport drives. The external disks and drives are connected only during the time the backup is run.

Miriam N. Jacobson

Your backup plan is an excellent one, but consider one addition. Make sure that you have four or more Passport drives just for your full weekly backup such that you have a rotation. A virus can remain dormant for longer than a week. It is still possible to get a virus under your plan.

I like to take old hard drives and use them for backups. Even a backup that is two or three months old can be a lifesaver after Crypto.

Mike Phillips, North Carolina

Thanks for the heads up on this. Just when I thought I finally had a good system of backup! I already backup to an external drive. However, I will re-think how I do that to protect my system.

Thank you,

Letisha Luecking Orlet, Illinois

Thanks I will have my computer nerd son set that up for me. Grateful for his taking care of mom. He makes fun of my lack of skills on the computer. But told me the company he worked for a fortune 500 company got hacked too. It is scary. The virus is NASTY.

Martha Jo Patterson, California

Prevention is also as important as backups. And you should encrypt all of your backups! You definitely don't want some dudes walking away with all of your client-confidential information!

(1) *Updates*. All of your computer systems should be routinely patched; in

other words, install Windows Updates. Update Java, Adobe Acrobat, and all the other programs on your computer. If you have a file server, that also has to be routinely patched.

(2) *Virus Scanners*. *All *computers should run a virus scanner. I personally use Norton Internet Security. Once a week, you should run MalwareBytes Anti-Malware. I run both programs in real time but I know other people have had problems in that configuration. Never had a problem with malware on my computer.

(3) *Don't Download Unknown Files*. I used to use Outlook with Google Apps but now I use the web interface. Google will run its own virus scans on attachments you receive or mail. It also will NOT allow you to send or email executable files that may install a virus on your computer. I don't know if Gmail does this through the Outlook interface, but the web interface stops dodgy files. It will actually warn me if it thinks an email is scammy.

(4) *Don't Download Unknown Files Redux*. I set up OpenDNS for my office. A DNS handles requests from your computer for websites. OpenDNS can be set up in your office router (and also to force every DNS request to go through its system). Requests to "bad" websites are blocked. You can configure the types of "bad" websites that will be blocked, such as porn, malware, etc. It will block some downloads from bad websites.

(5) *Two-Factor*. If you use Google Apps for Business, I recommend configuring the two-factor authentication and getting the FIDO U2F key. This will be a bit of a pain to set up, and you will need to have your phone or U2F key to log in. However, once it is configured, your email

account is pretty much unhackable. The hacker will not only need to know your password, but will also need to have your phone or U2F key or an emergency password you printed out and locked in your office file cabinet.

You should definitely have your son look into these measures. =) I think that he would know how to configure these products. Essentially, these are "set and forget" measures.

Yours,
William Chuang, New York

Wow thanks, I will print out and give to my tech guys (son and hubby). Hope others head your advice.

Martha Jo Patterson

Even cops sometimes pay CryptoLocker ransom

http://www.networkworld.com/article/2906983/security0/massachusetts-police-department-pays-500-cryptolocker-ransom.html or http://bit.ly/1aHWaFQ

James S. Tyre, California

Any suggestions about what to use to encrypt the computer and the backups? I used True Crypt for my computer, but understand it isn't available or recommended now. So what does everyone suggest?

Sincerely yours,
Michael D. Caccavo, Vermont’

I have TPM on my computer so I use BitLocker. Shrugs. TrueCrypt 7.1a was audited and found okay. Two projects took over the TC code base, so you can explore those options.

William Chuang
