Windows Secrets
Everything Microsoft forgot to mention

CryptoLocker: A particularly pernicious virus

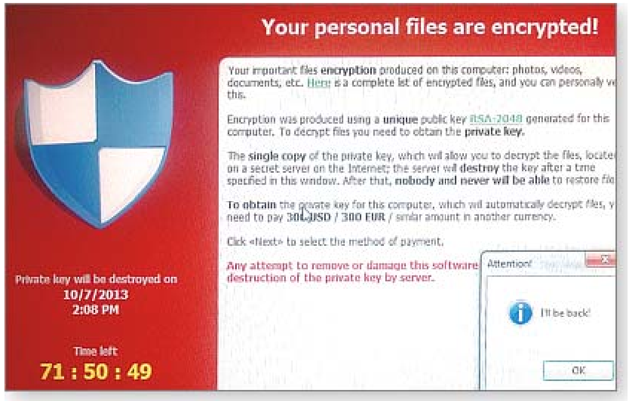
By Susan Bradley on October 24, 2013 in Top Story

Online attackers are using encryption to lock up our files and demand a ransom — and AV software probably won't protectyou.

Here are ways to defend yourself from CryptoLocker — pass this information along to friends, family, and business associates.

Forgive me if I sound a bit like those bogus virus warnings proclaiming, "You have the worst virus ever!!" But there's a new threat to our data that we need to take seriously. It's already hit many consumers and small businesses. Called CryptoLocker, this infection shows up in two ways.

First, you see a red banner (see Figure 1) on your computer system, warning that your files are now ***encrypted*** — and if you send money to a given email address, access to your files will be restored to you.



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally ve this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, locate on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore file

To obtain the private key for this computer, which will automatically decrypt files, y need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software destruction of the private key by server.

Private key will be destroyed on
10/7/2013
2:08 PM

Time left
71 : 50 : 49

Attention!

I'll be back!

Figure 1. CryptoLocker is not making idle threats.

The other sign you've been hit: you can no longer open Office files, database files, and most other common documents on your system. When you try to do so, you get another warning, such as "Excel cannot open the file [filename] because the file format or file extension is not valid," as stated on a TechNet MS Excel Support Team blog.

As noted in a Reddit comment, CryptoLocker goes after dozens of file types such as **.doc, .xls, .ppt, .pst, .dwg, .rtf, .dbf, .psd, .raw, and .pdf.**

CryptoLocker attacks typically come in three ways:

1) Via an email attachment. For example, you receive an email from a shipping company you do business with. Attached to the email is a **.zip** file. Opening the attachment launches a virus that finds and encrypts all files you have access to — including those located on any attached drives or mapped network drives.

2) You browse a malicious website that exploits vulnerabilities in an out-of-date version of Java.

3) Most recently, you're tricked into downloading a malicious video driver or codec file.

There are no patches to undo CryptoLocker and, as yet, there's no clean-up tool — the only sure way to get your files back is to restore them from a backup.

Some users have paid the ransom and, surprisingly, were given the keys to their data. (Not completely surprising; returning encrypted files to their owners might encourage others to pay the ransom.) This is, obviously, a risky option. But if it's the only way you ***might*** get your data restored, use a ***prepaid debit card*** — not your personal credit card. You don't want to add the insult of identity theft to the injury of data loss.

In this case, your best defense is prevention

Keep in mind that antivirus software probably won't prevent a CryptoLocker infection. In every case I'm aware of, the PC owner had an up-to-date AV application installed. Moreover, running Windows without admin rights does not stop or limit this virus. It uses social engineering techniques — and a good bit of fear, uncertainty, and doubt — to trick users into clicking a malicious download or opening a bogus attachment.

Your best prevention is two-fold:

1) Basic method: Ensure you keep complete and recent backups of your system. Making an image backup once or twice a year isn't much protection. Given the size of today's hard drives on standalone PCs, an external USB hard drive is still your best backup option. A 1TB drive is relatively cheap; you can get 3TB drives for under U.S. $200. For multiple PCs on a single local-area network, consider Michael Lasky's recommendations in the Oct. 10 Best Hardware article, "External hard drives take on cloud storage."

Small businesses with networked PCs should have automated workstation backups enabled, in addition to server backups. At my office, I use Backup Box by Gramps' **Windows Storage Server 2008 R2 Essentials** (site). It lets me join the backup server to my office domain and back up all workstations. I run the backups during the day, while others in the office are using their machines — and I've had no complaints of noticeable drops in workstation performance.

The upcoming release of Windows Server 2012 R2 Essentials (site) will also include easy-to-use, workstation-backup capabilities. Recently announced Western Digital drives will also act as both file-storage servers and workstation-backup devices.