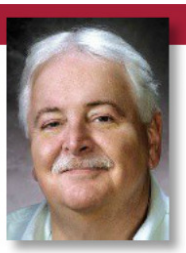


Steve Ford, WB8IMY, wb8imy@arrl.org

The Scourge of Ransomware

One fine morning you stroll into your station and fire up your computer. Your e-mail software starts and it suddenly alerts you to an incoming message. The message is from Federal Express and it states that you have an unpaid invoice for shipping charges. Federal Express has also helpfully included a copy of the invoice as a file attachment.

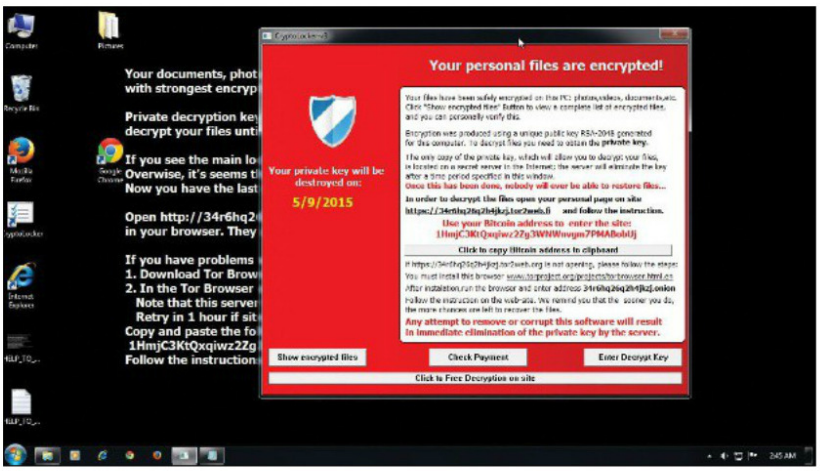
This is puzzling. You haven't shipped anything with Federal Express in recent memory. Surely this must be a mistake. Better check that invoice, right?

You open the file attachment, but the invoice doesn't seem to contain much relevant information. You shrug your shoulders and decide that Federal Express must have sent the e-mail in error. A click of your mouse deletes the message, and you go on about your business. If you had glanced at the LEDs on your computer, you may have noticed what appeared to be rapid flickering of the hard drive indicator. But chances are, you won't notice, and even if you did, by the time you chose to investigate, it would be far too late.

Within minutes you will be presented with a screen similar to the one shown here. Alternatively, you may also see a display stating that the FBI, CIA, or some other government agency has taken over your computer due to an alleged violation of the law. Either way, the effect is the same: All of your files — videos, family photos, financial records, Amateur Radio logs, etc — have been locked. You cannot gain access to your files unless you pay a ransom, and you must do so before a given date.

Files Held Hostage

Welcome to the world of *ransomware*. The ransomware gained access to your computer the moment you opened that file attachment. The attachment contained what is known as a *payload*. Some ransomware payloads lock down your computer, often by modifying your hard drive's master boot record or partition table. The more sophisticated payloads go much further by encrypting all of your files. At the time this column was written, encrypting payloads appeared to be the weapons of choice, with Cryptolocker being among the most common.



When ransomware strikes, you may see a screen similar to this one.

Of course, your initial response will be to think that you can somehow rid your computer of the virus. Good luck with that. Payloads such as Cryptolocker use what is known as *strong encryption* that is virtually unbreakable because only the ransomware author has the key.

Worse still, many ransomware applications are smart enough to encrypt not only the hard drives in your computer, they will also search for files that may be on other computers in your home network and they will even encrypt files that you have stored in cloud services such as Dropbox. Like most victims, you will quickly come to the realization that you have no choice except to pay the ransom.

But if you pay the ransom, what assurance do you have that the criminals will give you the code to unlock your files? The answer is that you have none. However, the vast majority of data kidnappers are true to their word, not because they have hearts of gold, but rather because doing otherwise would be bad for business. If the kidnappers didn't release the unlocking code upon receiving the ransom, the news would spread rapidly and victims would soon refuse to pay; the scam would no longer work.

Don't Become a Victim

- If you haven't already done so, install antivirus software on your computer and keep it up to date. If you are a *Windows 10* user, the good news is that antivirus software is included in the operating system, and Microsoft does a reasonably good job of keeping it current.

- Never open an e-mail attachment from someone you don't know, or from a company with whom you have not done business. Be suspicious of e-mail attachments in general. If your gut tells you that an e-mail is potentially bogus, it probably is. For example, the Internal Revenue Service will never send you an e-mail with a file attachment. Neither will ARRL, unless it is a file that you already expect us to send, or have specifically requested. (*QST* authors receive PDF files of their articles, for instance.)

- Finally, back up all of your files on a regular basis, but use a USB external hard drive or similar device that you can unplug from your computer when the backup is complete. Ransomware can't encrypt files it can't reach!