CryptoLocker Ransomware. What is it?

Ransomware is a type of malware that prevents or limits you from accessing your system. This type of malware forces victims to pay a 'ransom' through online payment methods in order to grant access to their systems, or to get their data back.

CryptoLocker is a ransomware Trojan which targets computers running Microsoft Windows and has been circulating since late 2013.

It is typically propagated as an attachment to a seemingly innocent e-mail message, which appears to have been sent by a legitimate company. A ZIP file attached to the email message contains an executable file with the filename and the icon disguised as a PDF file.

With Windows' hidden extensions feature, the sender has named their file with ".pdf" at the end (Windows hides the .exe) and the unwitting user is fooled into thinking the attachment is a harmless PDF file from a trusted sender.

Once CryptoLocker is in the door, it targets files with the following extensions:

*.odt, *.ods, *.odp, *.odm, *.odc, *.odb, *.doc, *.docx, *.docm, *.wps, *.xls, *.xlsx, *.xlsm, *.xlsb, *.xlk, *.ppt, *.pptx, *.pptm, *.mdb, *.accdb, *.pst, *.dwg, *.dxf, *.dxg, *.wpd, *.rtf, *.wb2, *.mdf, *.dbf, *.psd, *.pdd, *.pdf, *.eps, *.ai, *.indd, *.cdr, *.jpg, *.jpe, img_*.jpg, *.dng, *.3fr, *.arw, *.srf, *.sr2, *.bay, *.crw, *.cr2, *.dcr, *.kdc, *.erf, *.mef, *.mrw, *.nef, *.nrw, *.orf, *.raf, *.raw, *.rwl, *.rw2, *.r3d, *.ptx, *.pef, *.srw, *.x3f, *.der, *.cer, *.crt, *.pem, *.pfx, *.p12, *.p7b, *.p7c

When it finds a file matching that extension, it encrypts the file using a public key and then makes a record of the file in the Windows registry under HKEY_CURRENT_USER\Software\CryptoLocker\Files. It then prompts the user that his or her files have been encrypted and that he or she must send hundreds of dollars to the author of the malware to retrieve and access the files again.

The success of CryptoLocker spawned a number of unrelated and similarly named ransomware Trojans working in essentially the same way, including some that actually refer to themselves as "CryptoLocker"—but are, according to security researchers, unrelated to the original CryptoLocker.

So what can you do?

As of now, your best bet is to prevent the infection in the first place. Once you're infected, your options for removing the infection involve time, money, data loss or all three.

Ensure you're backing up your files regularly. This way, if you do get infected you don't have as much at risk.