CryptoLocker is a ransomware virus believed to have first been posted to the Internet on 5 September 2013. CryptoLocker propagated via infected email attachments, when activated; the malware encrypts certain types of files stored on local and mounted network drives using RSA public-key cryptography. The malware then displays a message which offers to decrypt the data if a payment (through either Bitcoin or a pre-paid cash voucher) is made by a stated deadline, and threatened to delete the private key if the deadline passes. If the deadline is not met, the malware offered to decrypt data via an online service provided by the malware's operators, for a significantly higher price in Bitcoin.

Although CryptoLocker itself is readily removed, files remained encrypted in a way which researchers considered infeasible to break.

Since the end of July, researchers at security defense biz Blue Coat have been tracking the spread of CryptoWall through online advertising networks; websites referring on visitors have been set up in India, Myanmar, Indonesia, France and other countries. According to Blue Coat, Yahoo!'s ad network is favored by the crooks because it has a huge reach – its ads appear on a large number of sites – and can therefore funnel more victims towards the exploit sites than shady ad slingers, which are much smaller.

CryptoLocker typically propagated as an attachment to a seemingly innocuous e-mail message, which appears to have been sent by a legitimate company. A ZIP file attached to an email message contains an executable file with the filename and the icon disguised as a PDF file, taking advantage of Windows' default behavior of hiding the extension from file names to disguise the real .EXE extension.

The virus encrypts files across local hard drives and mapped network drives with the public key, and logs each file encrypted to a registry key. The process only encrypts data files with certain extensions, including Microsoft Office, OpenDocument, and other documents, pictures, and AutoCAD files. The payload displays a message informing the user that files have been encrypted, and demands a payment of 400 USD or Euro through an anonymous pre-paid cash voucher (i.e. MoneyPak or Ukash), or an equivalent amount in Bitcoin (BTC) within 72 or 100 hours (while starting at 2 BTC, the ransom price has been adjusted down to 0.3 BTC by the operators to reflect the fluctuating value of Bitcoin), or else the private key on the server would be destroyed, and "nobody will be able to restore files." Payment of the ransom allows the user to download the decryption program, which is pre-loaded with the user's private key. Some infected victims claim that they paid the attackers but their files were not decrypted.