CryptoLocker ransomware

The ransomware is a kind of computer virus (also known as malicious software). If the ransomware infects a computer then it demands money (also called ransom) from the victim. One of the ransomwares is the CryptoLocker. I think CryptoLocker is the most dangerous of all the computer viruses because it encrypts all important files on all attached storage devices of the infected PCs.

First version of CL has been spreading by spam- or zip file attachment mainly, or it is able to infect by visiting malicious websites. The newer versions of CL is able to infect through the mobile storage media, eg. flash drive. According to DataRecovery Ltd. the CryptoLocker has already infected more than half a million computers in all of Europe. The CryptoLocker uses RSA algorithm with 2048 bits strong encryption thus it is impossible to breake it and recover the encrypted files without the appropriate private key. With the public key it encrypts the files and only the private key is able to decrypt the encrypted files (with the best technique of our age). The victim can pay for the private key, if not then the data will be unreadable forever. If there is no up-to-date backup for his/her irreplaceable files and he/she would like to get back all data then the person has to purchase some bitcoins from the attacker for a private key. One bitcoin equals 600 Euros.

In this slide can be seen that they demand a half bitcoin for the unique private key. The CryptoLocker encrypts not only the contents of the internal HDDs but it encrypts all files on attached external data storage devices, i.e. Windows or Netware servers mapped drives, USB sticks, flash memories etc...

At my workplace at the Semmelweis University Faculty of Pharmacy I have found an infected laptop by CryptoLocker. The Symantec Endpoint Protection didn't detect any problem but all files had been encrypted on my professor’s laptop.
In spite of the infection the Symantec Endpoint Protection has confirmed that: "Your computer is protected". After the CryptoLocker had encrypted all data it emerged a pop-up window to inform about the infection and possibilities. On the window there was a timer that was counting down from 72 hours to zero. It was a serious threat.
If you don’t pay sooner than 72 hours then they would delete the private key (from their server) and your files would be lost forever because without it is not able to recover any of your personal files.

Unfortunately, my professor didn't have an up-to-date backup for his files therefore he was very upset. I tried to explain him if he would like to read any of this documents or to see any of his pictures then he should pay the ransom.
Some of encrypted file types by CryptoLocker: e.g. for Wordprocessor: doc, docx, rtf, wri, txt, or for Spreadsheet xls, xlsx, or for PowerPoint presentation: ppt, pptx, Adobe pdf, etc..

To prevent infection we mustn’t open any zip-attachment from unknown e-mail senders, we shouldn’t visit warez and other suspicious webpages, the Windows operating system should be updated and finally but not beside the point we need mostly an effective security software (i.e. Webroot with rollback function). According to my experiences: usually the users didn’t have an up-to-date backup for their important data, virus scanning software can’t restore the encrypted files and finally the saddest thing without a private key to restore the encrypted files are impossible.

Written by Tamás Ludman

Budapest, 12th of May 2014