CryptoLocker

Security

CryptoLocker is the latest big news in the Windows-based malware department. Here are the important parts of what I know about this bad boy.

- What CryptoLocker does:
  - It will encrypt all "user files" that it can see with professional-grade asymmetric encryption. "User files" are defined as those that have a large number of extension, including doc, docx, xls, xlsx, ppt, pptx, jpg, and many more.
    - Asymetric encryption uses one key to encrypt a file and requires a second key to decrypt the file. The encryption key is on your computer, but the criminal source of the malware retains the decryption key for a limited time, hoping that you'll pay to obtain that key.
  - It will attempt to encrypt files on the local hard drive as well as on any remote drives attached to the infected machine. This includes network shares, external hard drives, USB sticks, etc.
  - It will display a banner on the screen with a count-down timer. When the timer expires, the decryption key stored by the criminal source is deleted.
  - The criminal hopes that you will "buy" the decryption key to recover your files. Currently, the charge is $300 and must be done within 72 hours of the infection. We do *not* recommend that you purchase the key.
- How CryptoLocker is delivered to your computer:
  - As an attachment to an email message. The most prevalent disguise I am hearing is that a zip file purporting to be a voice mail message is received. The zip file contains a dropper program that retrieves CryptoLocker from the network.
  - Possibly as a drive-by attack from a malicious website.
- Is there any good news?
  - Most AV software is identifying at least some variants of CryptoLocker and disabling it. However, AV is a game of whack-a-mole that the AV software can't win as long as the criminals behind the malware are finding it profitable.
- What should you do now?
  - BACK UP YOUR PERSONAL FILES! But don't leave the backup drive attached to the computer if you simply copied your files to the external drive. They'll be encrypted, too.
  - Don't open unexpected attachments in email.
  - Don't click on links in email unless you are certain of where the link will take you and what you'll find there.
- What should you do if you become infected?
  - If the banner with the countdown timer has appeared, cease using the computer and shut it down. Contact your IT support team and the ITS Security Office.
  - If the banner has not yet appeared, but you believe you have triggered CryptoLocker, PULL THE POWER CORD. The encryption happens one file at a time and the sooner the malware stops running, the fewer files encrypted. Contact your IT support team and the ITS Security Office.