CryptoWall Ransomware

CryptoWall and its variants is one of the most devilishly clever viruses released thus far. It gets into your Windows computer typically via an email attachment disguised as a normal PDF file, from infected websites, and from ad sites. The virus does not work on Mac computers. Once installed on your computer, it proceeds to encrypt all your data files in a way that can only be reversed by purchasing a private key and decryption application to decrypt all your data files. In other words, you are held ransom until you pay to decrypt. The ransom amount starts at $500 and if not paid within three days doubles to $1000. You have about a week, after which the possibility to decrypt your data goes away, making your files unrecoverable. The ransom is only accepted in Bitcoins, a digital currency that is difficult to procure.

If you do get infected and have automated file level backup (as most people do), it is probable that the backup copies of your files will also be encrypted.

There are two telltale signs that indicate CryptoWall is in your computer:

- When attempting to open certain files, such as .doc, .xls or .pdf, for example, the files are launched with the correct program; however, data may be garbled or not properly displayed. Additionally, an error message may be accompanied when trying to open infected files.
- The most common indication will be the appearance of three files at the root of every directory that contains files that were encrypted by CryptoWall.
    - DECRYPT_INSTRUCTION.txt
    - DECRYPT_INSTRUCTION.html
    - DECRYPT_INSTRUCTION.url

Clicking on any of these files left behind in the wake of CryptoWall's infection will lead you to step-by-step instructions necessary to carry out the ransom payment.

To date, I am aware of three instances within the last two months of CryptoWall getting into my customer's computers:

- Customer 1 chose to not pay the ransom and walked away from all their data
- Customer 2 paid the ransom. The effort to make the payment in Bitcoins and to run the decryption application cost them a week in down time, but all the data was recovered
- Customer 3 had an external monthly system image that they were able to recover to, costing them three weeks of lost work since the infection occurred in the third week of the month

Because there are so many variations, antivirus vendors have not yet been able to provide protection. There is one IT firm that I have found that has developed an application to help block infection. It is called CryptoPrevent and is available from FoolishIT.com. One can choose the free version which requires one to manually keep the product updated or one can purchase CryptoPrevent Premium for $15.00 to have automated updates.

While it is unusual to install software to protect against just one virus, I believe in this case it is warranted because the impact of getting this virus can be potentially devastating.

To protect you as much as possible from this terrible virus, I strongly recommend you install CryptoPrevent and set up automatic monthly system image creation to an external hard drive, keeping at least two months of images available. If you do not already have an external hard drive, a 1 TB drive can be purchased for about $80.00.

If you would like me to perform these tasks for you, please make an appointment ASAP!

This newsletter, as well as all past newsletters, can be found on my web site (http://steve.gimnicher.com).