NOTICE

CryptoLocker Ransomware is spreading rapidly across the internet. There is no cure. We have local reports of users becoming infected by clicking on attachments that often "appear to be coming from inside the organization". Zip files are especially suspect. It seeks out all files on all shares that you have full rights to and encrypts them. Removal of Cryptolocker is not hard, but the encrypted files are not retrievable without paying the ransom. If you have the files backed up, you can remove the infection and restore from backups.

You MUST tell your users to immediately stop clicking on any attachments that they cannot verify the source through some other means (i.e. you know the person sent this to you because they told you). If you have IDs with full rights to your network, you are in big trouble, if one of your users gets this infection. Physically remove the computer from the network ASAP.

We are investigating this further and will have more information as it becomes available.

Below is a brief overview of CryptoLocker:

CryptoLocker is a ransomware program that was released around the beginning of September 2013. This ransomware will encrypt certain files using a mixture of RSA & AES encryption. When it has finished encrypting your files, it will display a CryptoLocker payment program that prompts you to send a ransom of either $100 or $300 in order to decrypt the files. This screen will also display a timer stating that you have 96 hours, or 4 days, to pay the ransom or it will delete your encryption key and you will not have any way to decrypt your files. This ransom must be paid using MoneyPak vouchers or Bitcoins. Once you send the payment and it is verified, the program will decrypt the files that it encrypted.