MASS CRYPTOLOCKER RANSOMWARE SPAMMING COMPUTER USERS

The United States Computer Emergency Readiness Team (US-CERT) and Britain's National Crime Agency (NCA) have both issued an "urgent alert" to computer users about the threat posed by the CryptoLocker Malware. They have warned that online criminals have launched a major internet attack designed to hold victims' computer data hostage, and demand a high ransom be paid. This alert warns that the CryptoLocker ransomware has been distributed via spammed-out emails claiming to come from banks and financial institutions.

WHAT IS CRYPTOLOCKER?

It's a Trojan horse that encrypts computer files and demands a ransom be paid for the decryption key. CryptoLocker targets computers running versions of windows. Once your computer is infected, CryptoLocker hunts for files to encrypt not just on your hard drive, but on any connected drives, including mapped network shares, and even folders that you might sync up with the Cloud – such as DropBox.

Once files have been encrypted, CryptoLocker displays a message that demands you electronically send the ransom payment (options may include Bitcoin, MoneyPak cashU, or UKash) in order to decrypt files. A 72 hour timer is displayed, which ticks down and explains that if you do not pay the ransom demand, your files will be permanently inaccessible and impossible to ever decrypt.

HOW IS CRYPTOLOCKER SPREAD?

It is typically distributed via spammed-out emails claiming to come from banks and financial institutions. If you click on the attached file (which might pretend at first glance to be a PDF file, but actually use the .PDF.EXE double extension trick to hide its executable nature), your computer becomes infected.

It is also possible for CryptoLocker to be distributed in other ways. For instance, by compromising websites with malicious exploit kits that take advantage of software vulnerabilities to install CryptoLocker on visiting computers.

HOW TO PROTECT YOURSELF AGAINST CRYPTOLOCKER?

Here are some precautions you should take to protect yourself against CryptoLocker:

- Keep your computer up-to-date with anti-virus and security patches.
- Be cautious of opening unsolicited email attachments or clicking on unknown links.
- Consider setting a software restriction policy on your Windows PCs that prevents executables from running from certain locations on your hard drive.
- Make backups of your important data and keep them separate from your computer (to prevent malware like CryptoLocker from encrypting your backups as well).

CryptoLocker is a serious threat. If you're unlucky enough to have your computer infected by it, and haven't taken precautions, you may find yourself in the unpleasant situation of having to choose whether to pay the ransom, or never gain access to your data again. Therefore, we recommend you take these precautions to better protect your important business data.