Public Service Announcement

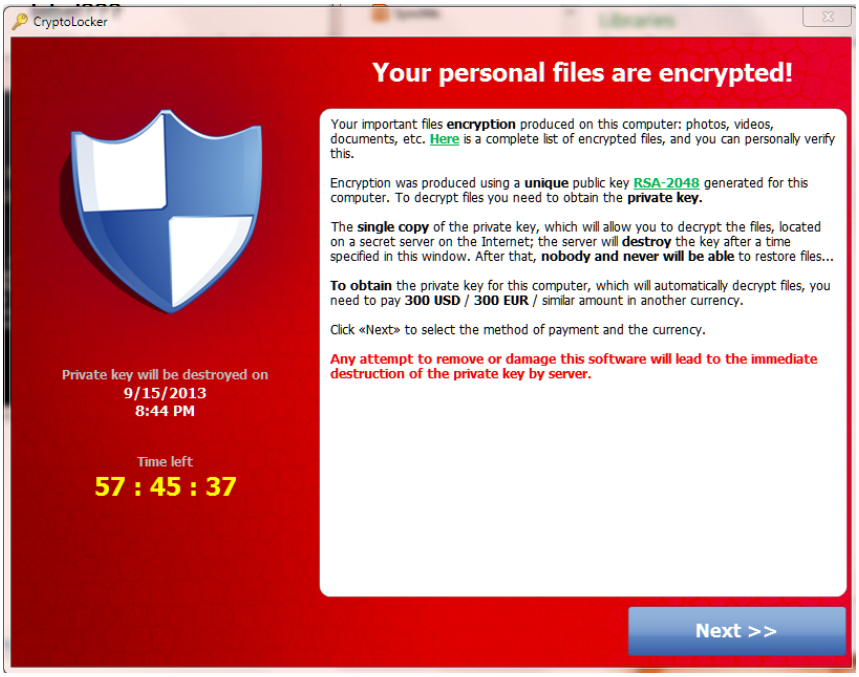
FEDERAL BUREAU OF INVESTIGATION

October 28, 2013

CRYPTOLOCKER RANSOMWARE ENCRYPTS USER'S FILES

The FBI is aware of a file-encrypting Ransomware known as CryptoLocker. Businesses are receiving emails with alleged customer complaints containing attachments that when opened, appear as a window that is in fact a malware downloader. This downloader installs the actual CryptoLocker malware.

The verbiage in the window states that important files have been encrypted using a unique public key generated for the computer. To decrypt the files you must obtain the private key. A copy of the private key is located on a remote server that will destroy the key after the specified time shown in the window. The attackers demand payment of a ransom ranging from $100 to $300 to decrypt the files.



*Unfortunately, once the encryption of the files is complete, decryption is not feasible. To obtain the file specific Advanced Encryption Standard (AES) key to decrypt a file, you need the private RSA key (an algorithm for public key cryptography) corresponding to the RSA public key generated for the victim's system by the command and control server. However, this key never leaves the command and control server, putting it out of reach of everyone except the attacker. The recommended solution is to scrub your hard drive and restore encrypted files from a backup.

As with any virus or malware, the way to avoid it is with safe browsing and email habits. Specifically, in this case, be wary of email from senders you don't know, and never open or download an attachment unless you're sure you know what it is and that it's safe. Be especially wary of unexpected email from postal/package services and dispute notifications.

If you have been a victim of an internet scam, please file a complaint at www.ic3.gov.

	*emsisoft.com; netlogicdc.com