New Site Recovers Files Locked by CryptoLocker Ransomware

Until today, Microsoft Windows users who've been unfortunate enough to have the personal files on their computer encrypted and held for ransom by a nasty strain of malware called CryptoLocker have been faced with a tough choice: Pay cybercrooks a ransom of a few hundred to several thousand dollars to unlock the files, or kiss those files goodbye forever. That changed this morning, when two security firms teamed up to launch a free new online service that can help victims unlock and recover files scrambled by the malware.

First spotted in September 2013, CryptoLocker is a prolific and very damaging strain of malware that uses very strong encryption to lock files that are likely to be the most valued by victim users, including Microsoft Office documents, photos, and MP3 files.

Infected machines typically display a warning that the victim's files have been locked and can only be decrypted by sending a certain fraction or number of Bitcoins to a decryption service run by the perpetrators. Victims are given 72 hours to pay the ransom — typically a few hundred dollars' worth of Bitcoins — after which time the ransom demand increases fivefold or more.

But early Wednesday morning, two security firms – Milpitas, Calf. based FireEye and Fox-IT in the Netherlands — launched decryptcryptolocker.com, a site that victims can use to recover their files. Victims need to provide an email address and upload just one of the encrypted files from their computer, and the service will email a link that victims can use to download a recovery program to decrypt all of their scrambled files.

The free decryption service was made possible because Fox-IT was somehow able to recover the private keys that the cybercriminals who were running the CryptoLocker scam used on their own (not free) decryption service. Neither company is disclosing much about how exactly those keys were recovered other than to say that the opportunity arose as the crooks were attempting to recover from Operation Tovar, an international effort in June that sought to dismantle the infrastructure that CryptoLocker used to infect PCs.

Full Story at: http://krebsonsecurity.com/2014/08/new-site-recovers-files-locked-by-cryptolocker-ransomware/