Background Facts

- Cryptolocker was distributed by GameOver Zeus/P2P-Zeus using the built in "user_execute" command by several of the affiliates involved (users of) in P2P-ZeuS.
- Cryptolocker was spread either unrestricted, but also in some cases to specifically: US, Canada, Great Britain, Australia and New Zealand.
- Countries targeted were likely based on language and prosperity.
- Cryptolocker was a very simple but also robust and well made tool that was impossible to revert, and cryptographically correct.
- By having multiple payment options and also different ways to reach the payment page, through both regular infrastructure and a Tor .onion hidden service, it was a more successful than most of the cryptography based ransomware.
- 1.3% of the victims have paid up.
- Amount paid varied between 300 and 500 USD. (unconfirmed if other amounts were asked over time)
- Total payments was around 3M USD over a period of 9 months. (Bitcoin fluctuations make it impossible to be exact)
- Between the 5th of September 2013 and the 30th of May 2014 (9 months) a total of 545146 infections took place.
- Over 60% (62%) of the infections took place in the US.
- The files were individually encrypted using AES symmetric encryption.
- The AES keys are encrypted using the public RSA key provided by the server, and each RSA encrypted AES key and other essential information are added to the encrypted documents and images of the victim.
- The RSA private key, of which the public key is derived, is generated on the Cryptolocker server and not sent out unless the ransom has been paid.
- Repeated takedown attempts and operations from security industry groups have had no lasting effect in the infection rates or effectiveness of Cryptolocker.