

Postale: chiusi falsi siti dell'Enel che nascondevano un virus informatico

Sono stati chiusi dalla polizia Postale 17 falsi siti dell'Enel nei quali era presente un noto virus del tipo malware, conosciuto come "CryptoLocker".

CryptoLocker è un trojan comparso intorno alla fine del 2013 che infetta i sistemi Windows, criptando i dati del malcapitato e richiedendo un pagamento per la decriptazione, in genere non meno di 300 euro.

La somma spesso doveva essere pagata in "Bitcoin", una moneta virtuale che non viene controllata da alcuna autorità centrale, ma viene gestita autonomamente attraverso i siti di cambio (oggi un Btc vale circa 220 euro).

Nelle ultime settimane si era incrementata la diffusione del virus inviato via mail dalla società "Enel SpA" che invitava l'utente a visitare un link in cui erano presenti i dettagli di una bolletta per la fornitura di energia elettrica.

Una volta "cliccato" sul link, si approdava ad un falso sito web di una società su cui era presente un pulsante tramite il quale scaricare il file della bolletta, ma in realtà tale pulsante consentiva il download del malware sui pc delle vittime.

Le segnalazioni, arrivate a www.commissariatodips.it e attraverso l'app gratuita per smartphone Commissariatodips online, hanno consentito di concentrare le indagini e scoprire i siti che sono risultati tutti collocati all'estero.

Infatti i siti sono risultati inseriti su server situati in Turchia e in Russia; così gli uomini della Postale hanno attivato la rete internazionale 24/7 High Tech Crime del G8 Gruppo Roma-Lione - per le emergenze di carattere informatico e per richiedere l'immediata chiusura.

Le indagini condotte a livello internazionale per identificare i responsabili sono portate avanti dalla polizia Postale anche grazie al contributo di Europol e Interpol.

30/07/2015