

Polizia di Stato

La Polizia Postale chiude 17 siti dell'Enel

La Polizia Postale che ha portato alla chiusura di 17 falsi siti dell'Enel all'interno del quale si celava un pericoloso malware che aveva mietuto vittime tra privati cittadini e soggetti pubblici. Nelle ultime settimane si era assistito ad un massiccio incremento della campagna di diffusione del malware noto come "Cryptolocker". CryptoLocker è un trojan comparso intorno alla fine del 2013 ed è una forma di ransomware che infetta i sistemi Windows, criptando i dati della vittima e richiedendo un pagamento per la decriptazione, in genere non meno di 300 euro. La somma spesso deve 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). La segnalazione di questa nuova campagna era giunta al sito www.commissariatodips.it che aveva immediatamente provveduto ad allertare la competente unità del Servizio Polizia Postale e delle Comunicazioni. In questa ultima versione, la minaccia si è presentata attraverso un considerevole invio di email apparentemente inviate dalla società "ENEL SpA" nelle quali si 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 della suddetta 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. E' da evidenziare che sia le email fraudolente sia i falsi portali web risultavano ben costruiti e le informazioni in essi contenute risultavano scritte in perfetto italiano. Di seguito l'elenco dei falsi siti ENEL ospitanti il malware:

enel24.net

enel24.org

enelservizio.com

enelservizio.net

enel24.com

enel-elettrico.org

enel-elettrico.com

enel-elettrico.net

enelelettrico.org

enelelettrico.com

enelelettrico.net

enel-italia24.net

enel-italia24.com

enelitalia-servizio.net

enelitalia-servizio.org

enelitalia-servizio.com

enelitalia.net

Alcuni dei siti suelencati, tutti collocati all'estero, risultavano attestati su server situati in Turchia e in Russia, pertanto grazie ad una pronta e capillare attività, anche in coordinamento con i competenti uffici di sicurezza informatica di ENEL, gli investigatori del Servizio Polizia Postale hanno provveduto ad attivare la rete internazionale *24/7 High Tech Crime* del G8 per richiederne la immediata chiusura. Infatti presso il Servizio Polizia Postale e delle Comunicazioni è attestato il punto di contatto del *Network 24/7 High Tech Crime* del G8 - Gruppo Roma-Lione - per le emergenze di carattere informatico. L'apporto fornito dai partner internazionali, in particolare dal *Department of Cybercrime della polizia turca* e dal *Dipartimento K del Ministero degli Interni russo*, è risultato determinante ed in poco tempo tutti i siti sono stati chiusi. Questa operazione ha costituito un'ulteriore, decisiva, azione di contrasto al pericoloso fenomeno dei ransomware la cui diffusione è in costante aumento in tutto il mondo.

30/07/2015