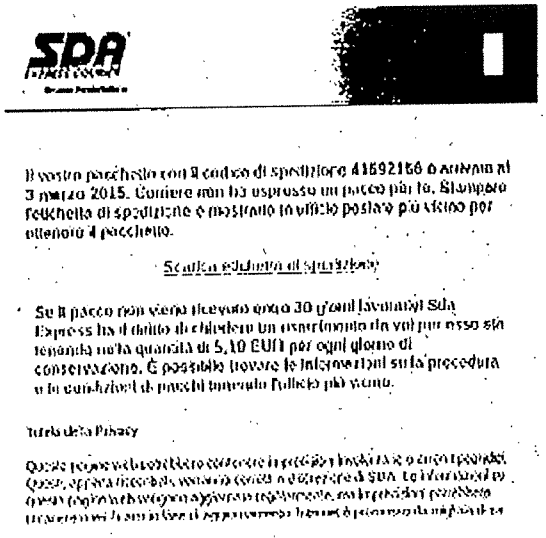
Attenzione al Cryptolocker
La Polizia di Stato mette in allerta gli utenti della Rete

Le numerose segnalazioni che giungono dagli internauti su questo nuovo virus che imperversa ormai da un po' di tempo sul web, ha indotto la Polizia di Stato ad aumentare le misure di prevenzione attraverso ogni strumento utile a garantire la sicurezza di chi naviga in Rete.

In tale contesto, la Polizia Postale e delle Comunicazioni ha concluso, proprio in queste ultime ore, un'operazione che ha permesso di sgominare un'organizzazione criminale per associazione per delinquere finalizzata all'accesso abusivo informatico, estorsione on line e riciclaggio degli illeciti proventi realizzati mediante la diffusione del virus "Cryptolocker", di cui sono rimaste vittima privati cittadini ma anche aziende, private e pubbliche.

Per quanto riguarda l'Emilia Romagna risultano denunciati alla Specialità oltre un centinaio di casi.

Un tipico scenario, che colpisce in particolar modo le aziende, è il seguente:
l'ignaro utente riceve una mail (apparentemente proveniente da noti vettori postali) che fornisce indicazioni su presunte spedizioni a suo favore.



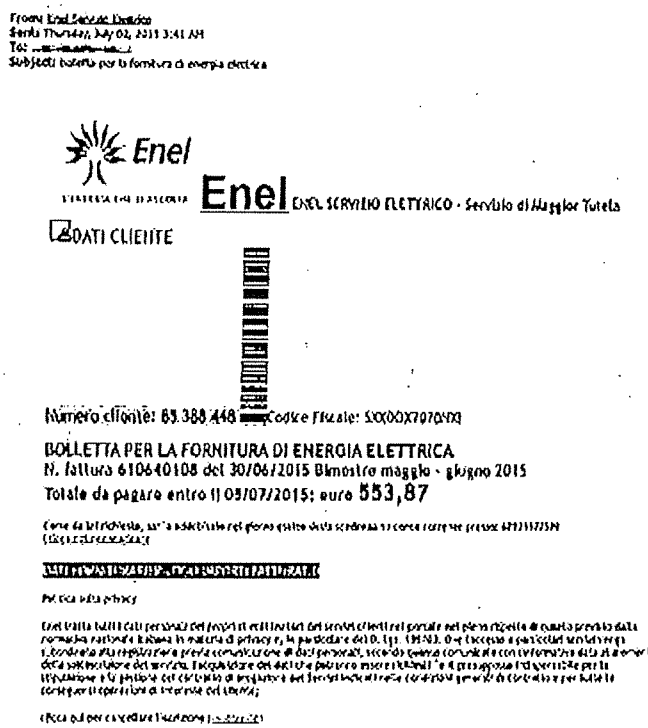
Il vostro pacchetto con il codice di spedizione 41692156 è arrivato il 3 marzo 2015. Corriere non ha lasciato un pacco per lei. Stampare ricevuta di spedizione e mostrarlo in ufficio postale più vicino per ottenere il pacchetto.

Scarica ricevuta di spedizione

- Se il pacco non viene ricevuto entro 30 giorni lavorativi Sda Express ha il diritto di chiedere un risarcimento da voi per esso sia rimasto nella quantità di 5,10 EUR per ogni giorno di conservazione. È possibile trovare le informazioni sulla procedura e le condizioni di pacchi tramite l'ufficio più vicino.

Tutela della Privacy

In altri casi, riuscendo a colpire sia aziende pubbliche che soggetti privati, la mail sembra provenire da fornitori di utenze o servizi (energia elettrica, acqua, gas etc.) oppure anche gestori di telefonia; il fittizio mittente può, infatti, essere mutato di volta in volta al fine di rendere più efficace l'inganno.



Enel

Enel ENEL SERVIZIO ELETTRICO - Servizio di Maggior Tutela

DATI CLIENTE

Numero cliente: 83 388 448 Codice Fiscale: SCOOOX707000

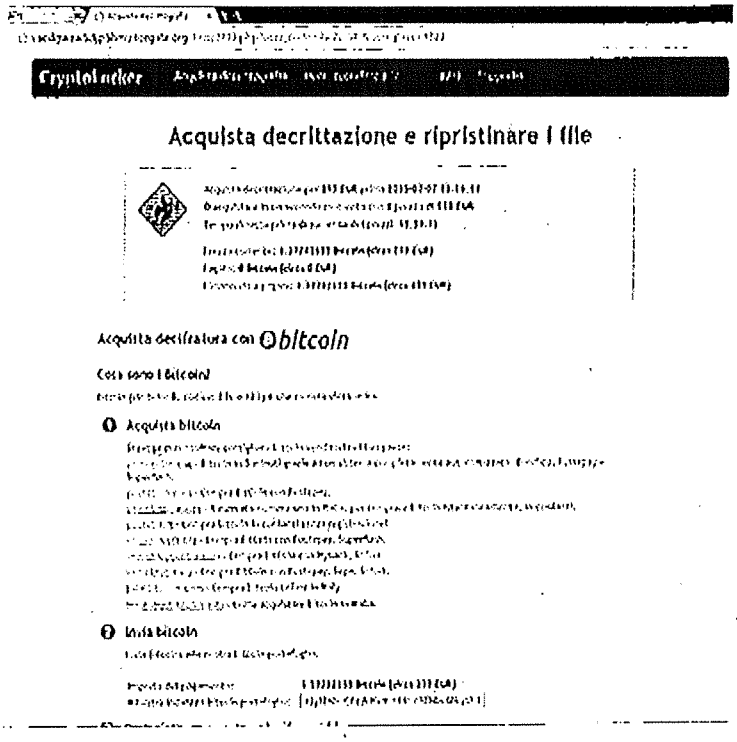
BOLLETTA PER LA FORNITURA DI ENERGIA ELETTRICA
N. fattura 610640108 del 30/06/2015 Bimestre maggio - giugno 2015
Totale da pagare entro il 05/07/2015: euro 553,87

Cliccando sul link contenuto nel corpo della mail oppure aprendo l'allegato (solitamente un documento pdf) viene iniettato un virus che inizia a criptare tutti i file contenuti nel computer, anche di quelli eventualmente collegati in rete e in tutte le periferiche ad essi connesse, inclusi quelli di backup se erroneamente tenuti collegati al sistema informatico.

A questo punto si realizza il ricatto dei criminali informatici che richiedono agli utenti, per riaprire i file e rientrare in possesso dei propri documenti, il pagamento di una somma di alcune centinaia di euro in bitcoin* a fronte del quale ricevere via e-mail un programma per la decriptazione.

** (Il Bitcoin è una moneta virtuale, esprimibile con un numero a 8 cifre decimali. Non esiste un'autorità centrale che la distribuisce e che ne traccia le transazioni in quanto le operazioni sono gestite collettivamente dal network attraverso dei siti c.d. exchanger che rilasciano monete virtuali incamerando moneta proveniente da carte di credito o altri strumenti elettronici di pagamento, ossia codici che a loro volta possono essere convertiti in denaro contante). Il valore di un BTC è stabilito dal mercato, come per ogni altro bene (attualmente 1 BTC corrisponde a circa 217 euro, ma tale valore è destinato ad aumentare, considerando che il numero massimo di BTC producibili attraverso il cd. processo di "mining" cui possono partecipare tutti i nodi della rete, è fissato a 21 milioni).*

Le schermate che vengono visualizzate sul dispositivo sono del seguente tenore:



ATTENZIONE
abbiamo criptato vostri file con il virus CryptOLOcker

I vostri file importanti (compresi quelli sui dischi di rete, USB, ecc): foto, video, documenti, ecc sono stati criptati con il nostro virus CryptOLOcker. L'unico modo per ripristinare i file è quello di pagare noi. In caso contrario, i file verranno persi.

Attenzione: La rimozione di CryptOLOcker non ripristinare l'accesso ai file crittografati.

Clicca qui per pagare per i file di recupero

Domande frequenti

[+] Che cosa è successo ai miei file?

Capire il problema

[+] Come faccio a ripristinare i miei file?

L'unico modo per ripristinare i file

[+] Cosa devo fare dopo?

Acquista decrittazione

[+] Non riesco ad accedere al tuo sito web, cosa devo fare?

Accesso specchi sito web utilizzando

E' importante non cedere al ricatto, anche perché non è certo che dopo il pagamento vengano restituiti i file criptati!

Le misure di sicurezza attuabili a difesa dei propri dati sono innanzitutto:

- controllare e leggere attentamente la posta in arrivo, se di dubbia provenienza o riferita ad una prassi non comunemente adottata dalle società o dalle persone con cui si è usualmente in contatto non aprire gli allegati e non cliccare sui link;
- installare e mantenere aggiornato un antivirus sui propri dispositivi;
- mantenere il firewall del dispositivo o della rete attivo;
- prestare attenzione durante l'installazione di software, in particolare le toolbar che, se provenienti da fonti non garantite possono celare insidie;
- predisporre dei backup dei file presenti sul proprio sistema informatico che, per dare garanzia di sicurezza, dovranno essere effettuati con frequenza e su supporti mantenuti scollegati dal sistema informatico.

Se ci si accorge di aver inavvertitamente aperto l'allegato della mail ingannevole, inoculando quindi il virus sul proprio dispositivo, spegnere immediatamente quest'ultimo (interrompendo anche l'alimentazione elettrica) così da inibire l'azione del cryptolocker che, se bloccato tempestivamente, non arriverà alla completa compromissione dei dati poiché la criptazione dei file non è affatto un processo immediato.

Per maggiori informazioni e assicurare un contatto diretto e continuativo con il cittadino, si può fare riferimento anche al **Commissariato di P.S. On-line**, per tutti coloro che frequentano la rete, caratterizzato da innovativi sistemi di interattività con l'utente, reperibile all'url: www.commissariatodips.it.

Il portale è stato appena integrato con apposita "app" scaricabile gratuitamente dal proprio smartphone o dall'ipad per consentire di venire incontro alle crescenti richieste di assistenza e di aiuto degli utenti della Rete, in tempo reale, e di conoscere sempre di più il mondo del web, i suoi rischi e le sue opportunità.