

CRYPTOLOCKER

L'attacco ai Vostri file

Che cos'è e come funziona

CryptoLocker è un pericolosissimo malware, molto potente, ovvero un "virus" di ultima generazione che prende in ostaggio i file sul computer che viene infettato (hard disk interni, hard disk usb esterni, chiavette usb e su dischi di rete e server) impedendone l'utilizzo.



Il suo scopo è di criptare i dati della vittima e richiedere un pagamento di ricatto per la decriptazione attraverso determinati metodi di pagamento on line, ma senza sicurezza di ripristino.

Il virus si riceve via Email, apparentemente lecita e inoffensiva, inviata da società legittime (es. Corriere SDA, Enel Spa, Apple, etc) o con nomi di persone conosciute e può essere presente in un file allegato, oppure un link di collegamento presente nel testo della Email, che farà scaricare il file "infetto".

Alcuni esempi di Email

Enel

ENEL SERVIZIO ELETTRICO - Servizio di Maggior Tutela
DATI CLIENTE
Numero cliente: 398 283 886
Codice Fiscale: AENAW6986JOY

BOLLETTA PER LA FORNITURA DI ENERGIA ELETTRICA
N. fattura 96120559 del 1/02/2016 Bimestre dicembre - gennaio 2015-2016
Totale da pagare entro il 1/02/2016: euro **773,62**

Come da lei richiesto, sar' a addebitato nel giorno esatto della scadenza su conto corrente presso: 448478737297
[Clicca qui per scaricare](#)

DATI FORNITURA RIEPILOGO IMPORTI FATTURATI/D



Il vostro pacchetto con il codice di spedizione 70592546 è arrivato al 22 giugno 2015. Corriere non ha espresso un pacco per te. Stampare l'etichetta di spedizione e mostrarlo in ufficio postale più vicino per ottenere il pacchetto.

[Scarica etichetta 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 sta tenendo nella quantità di 7,45 EUR per ogni giorno di conservazione. È possibile trovare le informazioni sulla procedura e le condizioni di pacchi tenendo l'ufficio più vicino.

I file colpiti sono normalmente documenti di Office (Word, Excel, PowerPoint, ecc), documenti PDF immagini, video.

Cryptolocker emerge alla fine del 2013, ed è una minaccia in continua evoluzione e mutazione e la sua diffusione è in progressivo aumento come la sua capacità di eludere i controlli di Anti-Spam e Anti Virus.

Come proteggersi???

Massima attenzione alle Email in arrivo, anche se per le capacità di evoluzione del virus come detto prima non è e non sarà di facile individuazione a volte. Basti pensare che sono molte le realtà nelle quali il virus ha colpito per la seconda o terza volta!!

Il Nostro consiglio è quello di adottare una corretta politica di gestione file, Backup e di Sicurezza per la propria struttura di rete.

La Tre Ci è in grado di valutare e studiare una soluzione personalizzata cliente per cliente valutando:

- ✓ Gestione dei File,
- ✓ Politica di Backup
- ✓ Protezione e sicurezza della propria rete,

A volte con piccoli accorgimenti ed una corretta gestione si può ovviare a problemi come quelli evidenziati in precedenza.

Il virus comporta una serie di problematiche che comportano dei costi indotti quali:

- ✗ Perdita dei file,
- ✗ Blocco del pc,
- ✗ Blocco della rete e server,
- ✗ Formattazione dei computer

Per informazioni

Tre Ci S.rl.

Marco De Vettor

Tel 0437 981054

Cel 320 7411515

Email m.devettor@tregrisrl.it