Ministero dell'Interno

Polizia di Stato

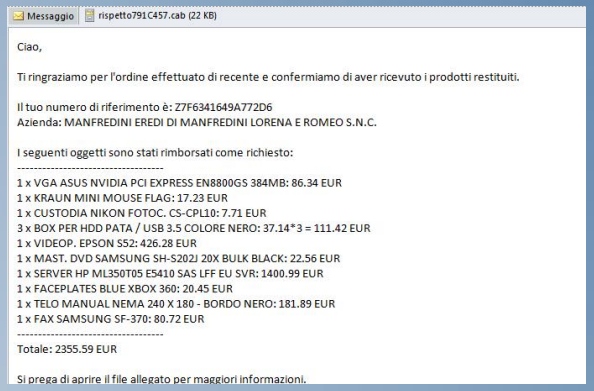
Compartimento Polizia Postale e delle Comunicazioni per l'Umbria

Cryptolocker

Perugia 10 luglio 2015

Ransomware

Un Ransomware è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in Inglese) da pagare per rimuovere la limitazione. Ad esempio alcune forme di ransomware bloccano il sistema e intimano l'utente a pagare per sbloccare del sistema, altri invece cifrano i file dell'utente chiedendo di pagare per riportare i file cifrati in chiaro.



In realtà il link o il file allegato non è altro che un modo per iniettare nel computer il virus CRYPTOLOCKER, così denominato perché cripta le memorie del computer rendendole indisponibili.

Enel
L'ENERGIA CHE TI ASCOLTA

ENEL SERVIZIO ELETTRICO - Servizio di Maggior Tutela
DATI CLIENTE
Numero cliente: 18 742 982
Codice Fiscale: SHCCFL3412SI

ADN KRONOS

BOLLETTA PER LA FORNITURA DI ENERGIA ELETTRICA
N. fattura 67447561 del 30/06/2015 Bimestre maggio - giugno 2015
Totale da pagare entro il 05/07/2015: euro 464,88

Come da lei richiesto, sar`a addebitato nel giorno esatto della scadenza su conto corrente presso: 462285832004
Clicca qui per scaricare

DATI FORNITURA | RIEPILOGO IMPORTI FATTURATID

In realtà il link o il file allegato non è altro che un modo per iniettare nel computer il virus CRYPTOLOCKER, così denominato perché cripta le memorie del computer rendendole indisponibili.

SDA EXPRESS COURIER
Gruppo Posteitaliane

Il vostro pacchetto con il codice di spedizione **49628714** è arrivato al **23 febbraio 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 6,14 EUR per ogni giorno di conservazione. È possibile trovare le informazioni sulla procedura e le condizioni di pacchi tenendo l'ufficio più vicino.

In realtà il link o il file allegato non è altro che un modo per iniettare nel computer il virus CRYPTOLOCKER, così denominato perché cripta le memorie del computer rendendole indisponibili.

Messaggio | rispetto791C457.cab (22 KB)

Ciao,

Ti ringraziamo per l'ordine effettuato di recente e confermiamo di aver ricevuto i prodotti restituiti.

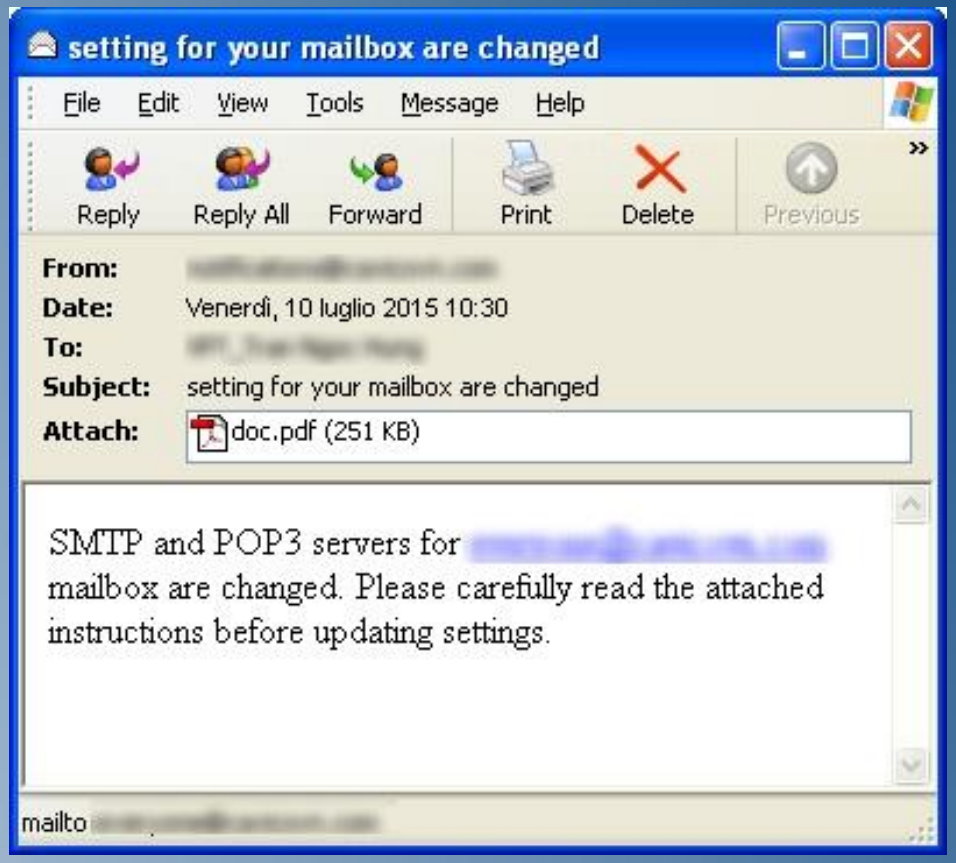
Il tuo numero di riferimento è: Z7F6341649A772D6
Azienda: MANFREDINI EREDI DI MANFREDINI LORENA E ROMEO S.N.C.

I seguenti oggetti sono stati rimborsati come richiesto:
---
1 x VGA ASUS NVIDIA PCI EXPRESS EN8800GS 384MB: 86.34 EUR
1 x KRAUN MINI MOUSE FLAG: 17.23 EUR
1 x CUSTODIA NIKON FOTOC. CS-CPL10: 7.71 EUR
3 x BOX PER HDD PATA / USB 3.5 COLORE NERO: 37.14*3 = 111.42 EUR
1 x VIDEOP. EPSON S52: 426.28 EUR
1 x MAST. DVD SAMSUNG SH-S202J 20X BULK BLACK: 22.56 EUR
1 x SERVER HP ML350T05 E5410 SAS LFF EU SVR: 1400.99 EUR
1 x FACEPLATES BLUE XBOX 360: 20.45 EUR
1 x TELO MANUAL NEMA 240 X 180 - BORDO NERO: 181.89 EUR
1 x FAX SAMSUNG SF-370: 80.72 EUR

Totale: 2355.59 EUR

Si prega di aprire il file allegato per maggiori informazioni.

In realtà il link o il file allegato non è altro che un modo per iniettare nel computer il virus CRYPTOLOCKER, così denominato perché cripta le memorie del computer rendendole indisponibili.



In realtà il link o il file allegato non è altro che un modo per iniettare nel computer il virus CRYPTOLOCKER, così denominato perché cripta le memorie del computer rendendole indisponibili.

A questo punto viene chiesto un riscatto che prevede il pagamento di una somma di alcune centinaia di euro in bitcoin, la moneta virtuale elettronica, per poter ricevere il programma di decriptazione.

L'immagine di sfondo del PC viene sostituita dall'immagine del CryptoLocker

ATTENZIONE: Cedendo al ricatto e pagando il riscatto non si ha alcuna garanzia di ricevere indietro o comunque di avere di nuovo accesso ai file criptati!

Come fare per difendersi

- ✓ tenere sempre aggiornato il software del proprio computer
- ✓ munirsi di un buon antivirus
- ✓ fare regolarmente il backup, cioè una copia dei propri file
- ✓ fare attenzione alle mail che ci arrivano, specialmente se non attese, evitando di cliccare sui link o di aprire gli allegati, perché è tramite la loro apertura che avviene la diffusione del virus.

Come fare se il PC è stato infettato

- ✓ Spegnere immediatamente il PC infetto
  (per interrompere la procedura crittografia di tutti i dati presenti)
- ✓ Non formattare l'hard disk

Ministero dell'Interno
Polizia di Stato

Commissariato di P.S. OnLine
www.commissariatodips.it

Nuova App
Commissariatodips Online