Cryptolocker

Il termine Cryptolocker viene utilizzato genericamente per identificare un ransomware (*ransom* in inglese significa *riscatto*) che ha come scopo infettare uno o più computer e i dispositivi collegati (compresi dispositivi rimovibili, unità di rete, …). Il Cryptolocker non attacca i file di sistema ma bensì i dati e cerca di colpirne il maggior numero possibile (ne esistono varie varianti che infettano solo le estensioni più comuni, quali doc, xls, pdf, jpeg, pst, ... e altre che le attaccano tutte). I dati non entrano mai in possesso del ricattatore e continuano a risiedere sul computer dell'infettato ma, mediante uno sofisticato software, l'hacker cripta i file e ne detiene la password necessaria per la decriptazione. Il ricattatore rilascerà il software contenente la password e l'applicativo di decriptazione solo a fronte del pagamento di un riscatto (solitamente in moneta virtuale BitCoin).

Come avviene l'infezione

Spesso l'infezione avviene mediante la ricezione di mail fraudolente riportanti intestazioni e loghi di società di primo piano (come Enel, TNT, SDA, DHL, Agenzia delle entrate, Poste Italiane, banche ecc.) accompagnate da un testo personalizzato con i dati del destinatario dell'email per trarlo maggiormente in inganno (se ad esempio scrivono a mario.rossi@dpconsulenze.com scriveranno Gentile Mario Rossi,…) e celano l'infezione in allegati (solitamente file EXE nascosti da icone o estensioni PDF, ZIP o RAR) o in link a siti esterni riportati nelle mail che puntano a siti realizzati agli scopi di avvalorare l'attendibilità della mail truffaldina e attivarne l'infezione.

Come evitare l'infezione

Diciamo che la risposta migliore è anche quella più ovvia: prestare molta attenzione e non aprire mail di cui non si conosce con certezza la provenienza (documentandosi prima su internet sull'attendibilità dell'indirizzo mittente), o che sono del tutto inattese. Per mail che già destano sospetteo si consiglia anche che la prima apertura avvenga su un dispositivo mobile, ad oggi immune, a questo attacco. Infine si consiglia di fare attenzione ai dettagli del testo contenuto nelle mail poiché spesso vi sono indizi che possono farvi evitare l'infezione (errori di digitazioni, errori di ortografia, italiano stentato o mal tradotto,…)
In caso di ulteriore incertezza potete anche inviarci la mail anomala, vi daremo riscontro appena possibile.

Cosa fare se si pensa di aver preso un cryptolocker

Quando si ha il sospetto che un pc potrebbe essere stato infettato da Cryptolocker si deve agire subito: provvedete quindi allo spegnimento anche forzoso (quindi mantenendo premuto il tasto di accensione) quando quest'ultimo impieghi più tempo del normale. Spegnete anche tutti gli altri computer della rete (server incluso) e scollegate i dischi USB o NAS collegati. Non perdete tempo! Meglio perdere qualche minuto che migliaia di file in più per uno spegnimento poco tempestivo.
Fatto questo contattateci con sollecitudine e attendete un nostro tecnico prima di procedere a qualsiasi riaccensione. Il nostro staff vi aiuterà nella verifica di quanto accaduto illustrandovi gli step necessari.

Cosa fare se si ha un cryptolocker

Purtroppo la criptazione dei dati è una procedura legale e ad oggi al mondo (nonostante le molte forze in campo, FBI e intelligence di tutto il mondo) non esiste una difesa in grado di evitare questa tipologia di infezione o procedura che possa restituirvi l'accesso ai vostri dati criptati dal virus.
In assenza di backup recenti purtroppo la scelta è solo tra: perdere i dati o pagare il riscatto per riaverli.
Se invece siete dotati di backup e quest'ultimo non fosse stato attaccato (i nostri uffici hanno recentemente testato delle nuove procedure, che ad oggi, sono in grado di difendervi dal cryptolocker) potrete riavere i vostri dati mediante un ripristino dall'ultimo backup.

Nelle pagine seguenti trovate esempi di alcune mail utilizzate per infettare i destinatari con Cryptolocker.

Esempi di mail con cryptolocker

Chiudi | Rispondi | Rispondi a tutti | Inoltra | Elimina | Spam | Azioni

Enel

L'ENERGIA CHE TI ASCOLTA.

ENEL SERVIZIO ELETTRICO - Servizio di Maggior Tutela

DATI CLIENTE

Numero cliente: [illegible]

Codice Fiscale: UXEBI59336NZ

[illegible]

BOLLETTA PER LA FORNITURA DI **ENERGIA ELETTRICA**

N. fattura **936925795** del 30/06/2015 Bimestre maggio - giugno 2015

Totale da pagare entro il 25/07/2015: **euro 546,80**

SDA EXPRESS COURIER

Gruppo Posteitaliane

Il vostro pacchetto con il codice di spedizione **G40633430** è arrivato al **21 ottobre 2014**. 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 4,75 EUR per ogni giorno di conservazione. È possibile trovare le informazioni sulla procedura e le condizioni di pacchi tenendo l'ufficio più vicino.

Tutela della Privacy

Informativa ai sensi dell'art. 13 del d. lgs n. 196 del 30 giugno 2003

I dati personali legittimamente acquisiti, a vario titolo, dalla SDA Express Courier S.p.A. potranno essere inseriti in apposite banche dati informatiche e cartacee nel rispetto delle disposizioni vigenti di cui al d.lgs n. 196/2003. Il mantenimento dei dati personali è finalizzato a permettere a SDA Express Courier S.p.A. di offrire agli utenti servizi commerciali personalizzati, consentendo agli stessi utenti di usufruire di servizi ulteriori e/o aggiuntivi, rispetto a quelli già utilizzati. I dati potranno essere comunicati a società controllanti, controllate o collegate, o comunque affidatarie di servizi per conto di SDA Express Courier S.p.A.

Questo è un messaggio generato automaticamente. Clicca qui per cancellarti.

Inoltra: [redacted] fattura n. 37257183 - Posta in arrivo

Messaggio

Elimina | Rispondi | Rispondi a tutti | Inoltra | Sposta | Regole | Indesiderato | Non letto | Categorizza | Completa

Inoltra: [redacted] fattura n. 37257183

[redacted]

Inviato: martedì 8 settembre 2015 16:27
A: Andrea Monguzzi (Flexxa Srl)

TELECOM ITALIA

Conto Telecom Italia n. 8/15

Fattura n.:	**WM31050900**
del:	31/08/2015
Codice Fiscale:	BGIOOO782268208H
Codice Segreto:	MQ 77297165
Il totale di euro:	**679.54**
`e da pagare entro il:	**31/09/2015**

DATI FORNITURA | RIEPILOGO IMPORTI FATTURA

Come lei ci ha chiesto, questo totale sar`a addebitato alla data di scadenza.
I suoi conti precedenti ci risultano pagati.Grazie.

Politica sulla privacy

La presente Privacy Policy ha lo scopo di descrivere le modalit`a di gestione di questo Sito, in riferimento all'uso dei cookie ed al trattamento dei dati personali degli utenti/visitatori che lo consultano.
I sito Internet Telecom Italia `e un servizio di informazioni on-line fornito da Telecom Italia S.p.A. ("Telecom Italia").Il suo utilizzo `e subordinato all'accettazione dei termini e delle condizioni qui di seguito stabiliti. Se non si intende accettare si `e invitati a non utilizzare il sito ed a non scaricare alcun materiale dallo stesso. Limiti all'utilizzo I contenuti delle pagine del sito Telecom Italia sono Copyright © di Telecom Italia S.p.A.. Tutti i diritti riservati. I contenuti delle pagine del sito Telecom Italia non possono, n'e totalmente n'e in parte, essere copiati, riprodotti, trasferiti, caricati, pubblicati o distribuiti in qualsiasi modo senza il preventivo consenso scritto di Telecom Italia, fatta salva la possibilit`a di immagazzinarli nel proprio computer o di stampare estratti delle pagine di questo sito unicamente per utilizzo personale. I marchi e loghi che compaiono su questo sito sono di propriet`a di Telecom Italia S.p.A. e delle sue affiliate (congiuntamente denominate "Gruppo Telecom Italia"). Essi non possono essere utilizzati su alcun sito Internet diverso dal sito Telecom Italia senza il preventivo consenso scritto di Telecom Italia S.p.A.. Il nome Telecom Italia e qualsiasi marchio che includa il marchio TELECOM ITALIA non possono essere utilizzati come indirizzi Internet di altri siti, o quali parti di tali indirizzi, senza il preventivo consenso scritto di Telecom Italia S.p.A.Qualsiasi materiale inviato a Telecom Italia, per esempio via e-mail o tramite le pagine World Wide Web, sar`a ritenuto di natura non confidenziale. Telecom Italia non avr`a obblighi di alcun tipo rispetto a tale materiale e sar`a libera di riprodurlo, usarlo, rivelarlo, mostrarlo, trasformarlo, farne opere derivate e distribuirlo a terzi, senza limiti. Inoltre, Telecom Italia sar`a libera di utilizzare tutte le idee, concetti, know-how o conoscenze tecniche contenute in tale materiale, per qualsiasi scopo, incluso, senza ad esso essere limitato, lo sviluppo, la produzione e commercializzazione di prodotti utilizzanti tale materiale. Chiunque invia materiale garantisce che il medesimo `e pubblicabile ed accetta di tenere indenne Telecom Italia da qualsiasi azione da parte di terzi in relazione a tale materiale. Cookies Un "cookie" (cio`e un piccolo data file che alcuni siti Web, mentre vengono visitati, possono inviare all'indirizzo del visitatore) pu`o trovarsi da qualche parte nel sito Telecom Italia, al fine di tracciare i percorsi del visitatore nel sito. Se si preferisce non ricevere cookies, si pu`o impostare il proprio browser in modo tale che vi avverta della presenza di un cookie e quindi decidere se accettarlo o meno. Si pu`o anche rifiutare automaticamente tutti i cookies, attivando l'apposita opzione nel browser. Legge e giurisdizione Queste condizioni sono regolate dalla legge italiana. Il Foro di Milano, Italia, avr`a giurisdizione e competenza esclusiva per eventuali controversie comunque connesse a queste condizioni. Ci`o nonostante, Telecom Italia si riserva, qualora lo ritenga necessario, di poter agire in giudizio di fronte a Tribunali di Paesi o citt`a diversi dall'Italia o da Milano, per proteggere i propri interessi e far rispettare i propri diritti..

Clicca qui per cancellare l'iscrizione.

Cryptolocker

From: Enel Servizio Elettrico
Sent: Thursday, July 02, 2015 3:41 AM
To: [redacted]
Subject: bolletta per la fornitura di energia elettrica

Enel
L'ENERGIA CHE TI ASCOLTA.

Enel ENEL SERVIZIO ELETTRICO - Servizio di Maggior Tutela

DATI CLIENTE

Numero cliente: 85 388 448 Codice Fiscale: SXXDOX7070NXI

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

Come da lei richiesto, sar`a addebitato nel giorno esatto della scadenza su conto corrente presso: 67923577579
Clicca qui per scaricare

DATI FORNITURARIEPILOGO IMPORTI FATTURATID

Politica sulla privacy

Enel tratta tutti i dati personali dei propri clienti fruitori dei servizi offerti nel portale nel pieno rispetto di quanto previsto dalla normativa nazionale italiana in materia di privacy e, in particolare del D. Lgs. 196/03. Ove l'accesso a particolari servizi venga subordinato alla registrazione previa comunicazione di dati personali, secondo quanto comunicato con l'informativa data al momento della sottoscrizione del servizio. l'acquisizione dei dati che potranno essere richiesti `e il presupposto indispensabile per la stipulazione e la gestione del contratto di erogazione dei Servizi indicati nelle condizioni generali di contratto e per tutte le conseguenti operazioni di interesse del cliente;

clicca qui per cancellare l'iscrizione (ususbscribe)