



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.





Ministero dell'Interno

Polizia di Stato



ENEL SERVIZIO ELETTRICO - Servizio di Maggior Tutela

DATI CLIENTE
Numero cliente: 18 742 982
Codice Fiscale: SHCCFL341251

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: 46285832004
[Clicca qui per scaricare](#)

[DATI FORNITURA](#) [RIEPILOGO IMPORTI FATTURATI](#)



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.

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 VIDEO, EPSON 552: 426.28 EUR
- 1 x MAST. DVD SAMSUNG SH-S2021 20X BULK BLACK: 22.56 EUR
- 1 x SERVER HP ML350T05 ES410 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 preza di aprire il file allegato per maggiori informazioni.



setting for your mailbox are changed

Repy Reply All Forward Print Delete Previous

From: [redacted]
Date: Venerdì, 10 luglio 2015 10:30
To: [redacted]
Subject: setting for your mailbox are changed
Attach: dccc.pdf (251 KB)

SMTP and POP3 servers for [redacted] mailbox are changed. Please carefully read the attached instructions before updating settings.

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.





Ministero dell'Interno

Polizia di Stato





ENEL SERVIZIO ELETTRICO - Servizio di Maggior Tutela

DATI CLIENTE

Numero cliente: 18.742.982

Codice Fiscale: SHCCFL341251

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 FATTURATI**

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.





Ministero dell'Interno

Polizia di Stato



SDA
EXPRESS COURIER
Gruppo Postale italiano



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.






Ministero dell'Interno

Polizia di Stato



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.





Ministero dell'Interno

Polizia di Stato



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.





Ministero dell'Interno

Polizia di Stato



CryptoLocker

Your personal files are encrypted!



Private key will be destroyed on
13/07/2015
12:37 PM

Time left:
72 : 34 : 50

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt the files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To **obtain** the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR / similar amount** in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Next >>

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.





Ministero dell'Interno

Polizia di Stato



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





Ministero dell'Interno

Polizia di Stato



CryptoLocker

Payment for private key

Choose a convenient payment method:
Bitcoin (most cheap option)



Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send below specified amount to Bitcoin address
1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh and specify the transaction ID, which will be verified and confirmed.

[Home Page](#)
[Getting started with Bitcoin](#)

Enter the transaction ID and press «Pay»:

2 BTC

<< Back PAY

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!





Ministero dell'Interno

Polizia di Stato

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.



Ministero dell'Interno

Polizia di Stato

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

Commissariato di P.S. online
Sportello per la sicurezza degli utenti del web

LIVELLO DI ALLERTA
ALTO per Hacking
ATTENZIONE! INVIO E-MAIL CON "ALLEGATO VIRUS CRYPTOLOCKER"

PROFILO NOTIZIE APPROFONDIMENTI DA SAPERE DOMANDE E RISPOSTE FORUM COLLABORA

Informati
Leggi le notizie per essere sempre informato sui reati telematici.
In primo piano
VIRUS
09.07.2015
ATTENZIONE! INVIO E-MAIL CON "ALLEGATO VIRUS CRYPTOLOCKER"
E' in atto l'invio di e-mail a privati cittadini ma anche aziende private e pubbliche, riguardanti indicazioni su presunte spedizioni effettuate o contenenti un link relativo a presunti acquisti on-line. [Continua...](#)
Archivio notizie

Domanda
Hai un dubbio? Compila il form qui sotto e chiedi ai nostri esperti.
Richiedi informazioni
Forum
Ultimo forum: [Le Frodi online](#)
Prossimo forum: **Attualmente non ci sono forum in programmazione**
[Registrati e partecipa](#)
Tutti i forum

Collabora
Se ti trovi in presenza di un reato informatico, **entra in contatto con noi.**
Segnala online
Denuncia per reati telematici
Denuncia per furto o smarrimento

polizia delle comunicazioni

- Presentazione
- Attività e organizzazione
- Storia
- Commissariato di P.S. on-line
- Centro Nazionale Contrasto Pedopornografia On-line
- Unità di analisi sul crimine
- CNAIPIC
- Collaborazione internazionale
- Iniziative
- Contatti
- Privacy Policy

Servizi

- Invia un quesito
- Partecipa al forum
- Segnala un reato
- Denuncia per reati telematici
- Ricerca sedi

Altri servizi

- Passaporto
- Stradale
- Stranieri
- Armi
- Moduli
- Servizi online

Ci trovi anche su Facebook

Una vita da social

Nuova App
Commissariatodips Online

