Oggetto:	ATTENZIONE - NUOVA ONDATA DI E-MAIL CON VIRUS CRYPTOLOCKER
Da:	noreply@istruzione.it
Data:	Lun, 18 Aprile 2016 12:13 pm
A:	scuole-nazionale@istruzione.it
Priorità:	Normale
Opzioni:	Visualizza l'intestazione completa | Visualizza versione stampabile | Scarica come file | View as plain text | Add to Address Book

Gentile utente,
in questi giorni sta raggiungendo livelli elevatissimi la diffusione di e-mail che potrebbero installare nel proprio computer una tipologia di virus altamente dannoso e non rilevabile da alcun antivirus tradizionale, il **CRYPTOLOCKER**.
In particolare tali e-mail in apparenza hanno come mittente **EQUITALIA**: in allegato (file Equitalia.jpg) una immagine che mostra come potrebbero apparire sul vostro client di posta elettronica.
Si raccomanda pertanto **di non aprire MAI gli allegati e non cliccare MAI i link** contenuti in e-mail provenienti da sconosciuti o di contenuto dubbio.

Le e-mail sospette potrebbero provenire da **mittenti vari (Istituti, Enti, gestori telefonici e fornitori di servizi ecc.)**, e contengono link e/o allegati che, una volta selezionati o aperti, installano nel proprio computer un virus in grado di criptare tutti i dati presenti all'interno dello stesso e nei dispositivi ad esso collegati.
Il virus si propaga tramite e-mail che possono arrivare all'indirizzo istituzionale *@istruzione.it* oppure ad indirizzi di posta privata a cui accedete via web dal vostro computer.
Cliccando sul link, oppure aprendo l'allegato, si attiva il virus che cripta i dati della vittima e richiede un pagamento per la loro decrittazione, oltre a propagarsi sugli altri dispositivi (chiavette USB, hard disk esterni, cartelle condivise in rete…): ecco perché questi virus, il più diffuso dei quali è**CryptoLocker**, sono noti col nome di *ransomware* (dall'inglese *ransom* = riscatto). Il pagamento tra l'altro non dà la certezza che i dati siano resi nuovamente fruibili.
In allegato (file *SchermateVirusCL.pdf*) ci sono alcuni esempi di schermate prodotte dal virus, dopo aver criptato tutti i file del pc.
Attualmente non esiste un software in grado di ripristinare i file criptati con le nuove varianti del CryptoLocker.

Al fine di arginare il fenomeno, si raccomanda di:
- non cliccare su link "sospetti": non farsi ingannare dal nome del link ma visualizzare l'indirizzo reale del sito passando - senza cliccare - col mouse sul link.
- non aprire file "sospetti"
- cestinare le e-mail "sospette": ad es. scritte con errori ortografici e grammaticali, in un italiano stentato, con richiesta di inserire PIN, password e dati personali su una pagina web (vedi allegato *EmailCL.png*)
- effettuare frequentemente il backup dei dati presenti sulla propria postazione, al fine di evitare la perdita degli stessi
- procedere comunque ad un costante aggiornamento del proprio antivirus

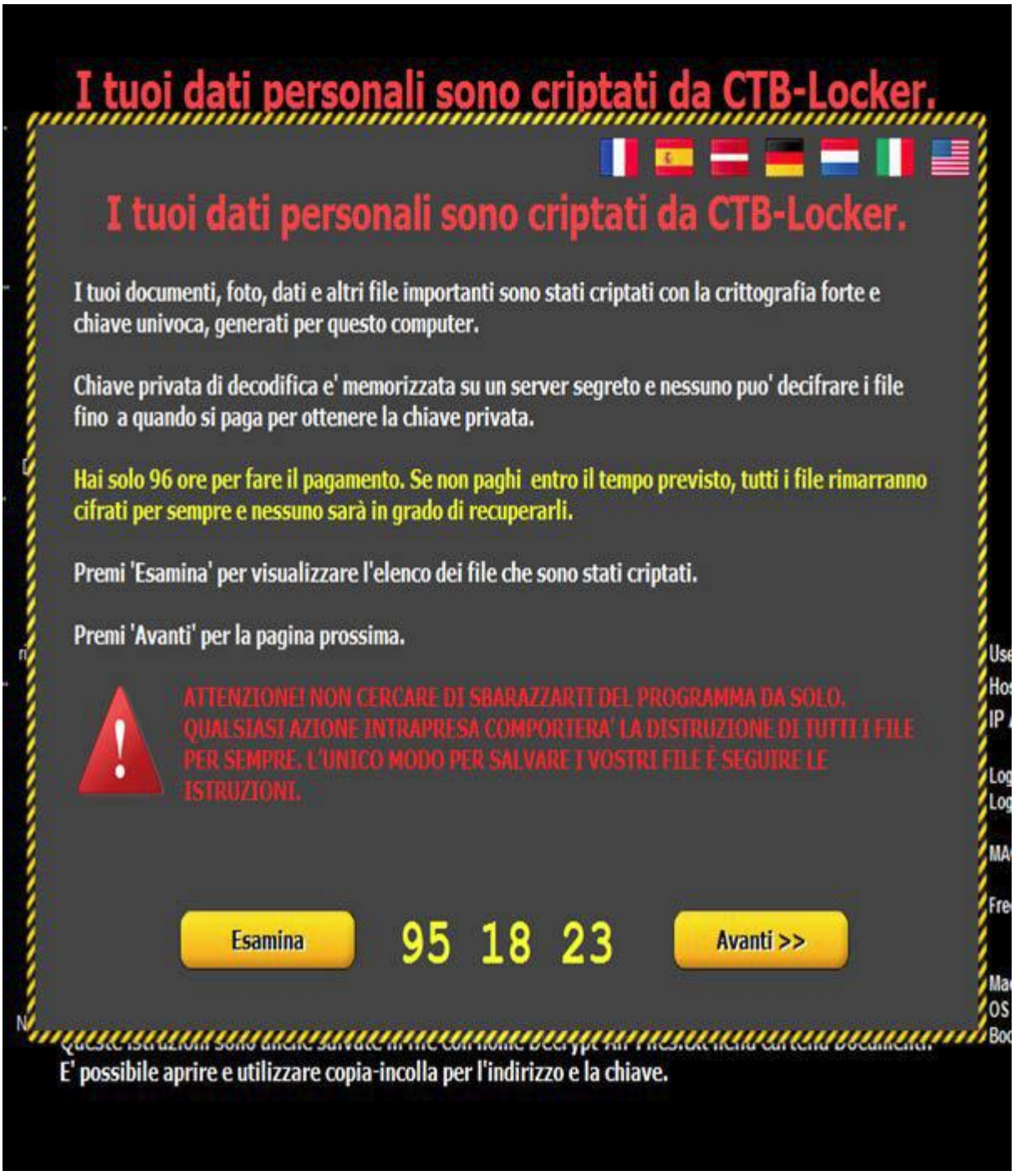
In caso di infezione, spegnere o disconnettere immediatamente il computer dalla rete, ed eventuali dispositivi ad esso collegati: quindi contattare la vostra assistenza tecnica.

Ministero dell'Istruzione, dell'Università e della Ricerca
D.G. Contratti, Acquisti, Sistemi Informativi e Statistica

Allegati:

untitled-[1.1].plain	**2.9 k**	[text/plain]	Download | Visualizza
SchermateVirusCL (1).PDF	**362 k**	[application/pdf]	Download
EmailCL (1).PNG	**1.6 M**	[image/png]	Download | Visualizza
Equitalia (1).jpg	**136 k**	[image/jpeg]	Download |

Esempi di schermate prodotte dal virus CryptoLocker



Esempi di mail contenente il virus

Da: servizioclienti@telecomitalia.it
Inviato il: 10-feb-2016 9.55
A: < @alice.it>
Cc:
Oggetto: Fattura TIM linea Fissa - Gennaio 2016 - scadenza 10/02/2016

Allegati:

Fattura 31433063982.zip (743K)

Gentile **@alice.it**,

ti informiamo che la tua fattura TIM di **Gennaio 2016** relativa alla linea **31433063982** è stata appena emessa ed è disponibile online.

Si prega di scaricare il fattura attaccato

Ti ricordiamo che in MyTIM Fisso nella sezioneIl mio profilo puoi richiedere di ricevere la **fattura TIM** esclusivamente online. **Risparmierai così le spese di spedizione postale**.

Ti aspettiamo presto su **www.tim.it**

Grazie

Servizio Clientitim.it

Attenzione:ti invitiamo a non rispondere a questo messaggio: questa casella di posta elettronica non è abilitata alla ricezione.

Esempi di mail contenente il virus

***** SPAM *** AVVISO NUMERO 00071552**

Equitalia <pagamento@gruppoequitalia.it>

Completare. Inizio fissato entro martedì 12 aprile 2016. Scadenza martedì 12 aprile 2016.

Categoria rossa

Inviato: martedì 12/04/2016 06:10
A: XXXXXXXX

Agente della Risossione
Equitalia S.p.A.
Via Cristoforo Colombo 751 - 0075197 - Roma

Art. 26 D.P.R. 29/09/1973, n. 602 e successive modifiche - Art. 60 D.P.R. 29/09/1973, n. 751, Art. 139 c.p.c.

Gentile XXXXXXXXXXXX@istruzione.it,

Il suindicato Agente della Riscossione avvisa, ai sensi delle intestate disposizioni di legge , di aver depositato in data odierna, nella Casa Comunale del Comune il seguente avviso di pagamento **"Documento Numero 00071552"** del 12/04/2016 , composto da 5 pagina/e di elenchi contribuenti a nr. 17 atti **[Scarica il documento]**

© Equitalia S.p.A. C.F. P.I. 0954689156751