didattica@maddalena-bertani.gov.it

Da: geic854002@istruzione.it
Inviato: lunedì 18 aprile 2016 15:36
A: didattica@maddalena-bertani.gov.it; dirigente; personale@maddalena-bertani.gov.it
Oggetto: I: ATTENZIONE - NUOVA ONDATA DI E-MAIL CON VIRUS CRYPTOLOCKER
Allegati: SchermateVirusCL (1).PDF; EmailCL (1).PNG; Equitalia (1).jpg

---

Da: noreply@istruzione.it [mailto:noreply@istruzione.it]
Inviato: lunedì 18 aprile 2016 12:13
A: scuole-nazionale@istruzione.it
Oggetto: ATTENZIONE - NUOVA ONDATA DI E-MAIL CON VIRUS CRYPTOLOCKER

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