Ministero dell'istruzione, dell'università e della Ricerca
Ufficio Scolastico Regionale per il Veneto
DIREZIONE GENERALE
Ufficio II - Ordinamenti scolastici. Politiche formative e orientamento. Rapporti con la Regione. Progetti europei. Esami di Stato.
Riva de Biasio – S. Croce 1299 - 30135 VENEZIA

Protocollo (vedasi timbratura in alto) Venezia, (vedasi timbratura in alto)

Ai Dirigenti Scolastici
delle Istituzioni Scolastiche di ogni ordine e grado del Veneto – Loro Sedi

Ai Responsabili della Sicurezza Informatica
Presso le Istituzioni Scolastiche di ogni ordine e grado del Veneto – Loro Sedi

OGGETTO: Misure e comportamenti per la prevenzione delle infezioni da virus Ransomware di computer e infrastrutture informatiche delle scuole

Si rende noto alle SS.LL. che il problema delle infezioni di computer, reti e sistemi informatici da virus denominati Ransomware (di recente ha avuto eccezionale diffusione quello chiamato WannaCry, https://it.wikipedia.org/wiki/WannaCry) sta coinvolgendo anche le Istituzioni Scolastiche.

Tali virus, sostanzialmente, "sequestrano" i file di dati attraverso una loro criptatura, per eliminare la quale viene richiesto l'invio di denaro ad un soggetto criminale (solitamente nella forma di bitcoin). La cifra è abbastanza modica per indurre al pagamento, ma esso non assicura di ricevere lo strumento di decriptazione per "liberare" i dati.

Si invita ad avere molta attenzione in merito in quanto i sistemi di rimozione sono parziali e a fine operazioni permangono danni e perdite. Di solito si rende necessario un ripristino da un backup sicuro (perdendo, ovviamente, gli ultimi file creati e modificati)
Peraltro, la diffusione di tali virus avviene per vie consuete: tipicamente, visite a siti internet infetti, e-mail di phishing con false fatture, bollette e avvisi di pagamento, ….

Si richiama quindi innanzitutto alla necessità di informare e formare tutto il personale sulle normali misure e comportamenti di sicurezza: aggiornamento del software, dal sistema operativo al browser, realizzazione di frequenti backup, utilizzo di antivirus di qualità, attenzione ai siti di cattiva reputazione (utilizzare le apposite estensioni dei browser per il controllo), non aprire allegati di e-mail di dubbia provenienza o di sconosciuti, … .

Sebbene le infezioni di questo tipo abbiano un po' più raramente come causa falle dei sistemi di rete, si invita comunque a curare con attenzione e continuità anche la sicurezza e la protezione dei dati nelle reti informatiche della scuola secondo norma e con i più aggiornati strumenti, sistemi e dispositivi.

Il Dirigente
Francesca Altinier

Firmato digitalmente da
ALTINIER FRANCESCA
C=IT
O=MINISTERO DELL'UNIVERSITA' E DELLA RICERCA/80185250588

Il referente
Franco Torcellan

Link interattivi alla pagina seguente

e-mail: direzione-veneto@istruzione.it - C.F. 80015150271 - PEC: drve@postacert.istruzione.it
Codice fatturazione elettronica: contabilità generale 9L2WQN - contabilità ordinaria HS9OVD
Codice IPA: m_pi - Codice AOO: AOODRVE
tel. 041/2723111

Ministero dell'istruzione, dell'università e della Ricerca
Ufficio Scolastico Regionale per il Veneto
DIREZIONE GENERALE
Ufficio II - Ordinamenti scolastici. Politiche formative e orientamento. Rapporti con la Regione. Progetti europei. Esami di Stato.
Riva de Biasio – S. Croce 1299 - 30135 VENEZIA

Si forniscono alcuni indirizzi di pagine web che trattano questo problema e descrivono modalità di prevenzione e di rimozione:

Wikipedia
https://it.wikipedia.org/wiki/Ransomware

Blog di Kaspersky

- https://blog.kaspersky.it/ransomware-for-dummies/9455/
- https://blog.kaspersky.it/tag/ransomware/

Norton by Symantec
https://it.norton.com/clubnorton-ransomware-tips

Ransomeware Blog
http://www.ransomware.it/

PC Risk
https://www.pcrisk.it/guide-per-la-rimozione/8385-satan-ransomware

The Windows Club
http://www.thewindowsclub.com/repair-master-boot-record-mbr-windows

No more ransom!
https://www.nomoreransom.org/