2022-01-28 17:36 (noreply@istruzione.it) - CSIRT-MI - Campagna phishing Emotet del 28/01/2022

Gentile Utente,

a seguito di analisi di questo CSIRT, si è rilevato che nella giornata di oggi lei potrebbe aver ricevuto nella sua casella postale mail a cui è stato aggiunto nell'oggetto uno o più dei seguenti suffissi "RE:" "RV:" "FW:" "Re:" "Tr:" "Rv:" ed al suo interno allegati con estensione xls oppure zip

Si tratta di una campagna di phishing molto aggressiva.
Le chiediamo di non ritenere attendibili tali mail e quindi eliminarle.

Nel caso in cui lei abbia proceduto per errore ad aprire l'allegato, le chiediamo di eseguire le seguenti azioni nell'ordine riportato:

• Scansione antivirus completa ed approfondita;
• Scansione con software (per esempio AdwCleaner) per l'individuazione di eventuali Adware, Toolbars, Potentially Unwanted Programs (PUP);
• Pulizia della cache del browser (su Chrome: impostazioni -> nella barra superiore di ricerca inserire "Cancella dati di navigazione" -> Cancella dati di navigazione -> Selezionare "Cronologia di navigazione", "Cookie e altri dati dei siti", "Immagini e file memorizzati nella cache" -> Cliccare su "Cancella dati");
• Controllo delle estensioni del browser per rilevare che non siano presenti estensioni non personalmente installate;
• Reset e cambio password della casella di posta istituzionale successivamente ai passi sopra menzionati.

Inoltre, alleghiamo le linee guida sull'uso corretto della postazione di lavoro e della casella di posta elettronica:

- 'CSIRT MI - Raccomandazioni di sicurezza per l'Utente - Smart Working_v1.0.pdf' e
- 'CSIRT MI - Raccomandazioni Sicurezza Posta Elettronica_v1.0.pdf'

Si ringrazia della collaborazione.

CSIRT MI