Da: noreply@istruzione.it
Oggetto: CSIRT-MIM - Campagna phishing Emotet del 23/03/2023
Data: 23/03/2023 12:45:43

Gentile Collega,

il CSIRT MIM ha evidenza di campagne malspam in corso che attenzionano questo Ministero e raccomanda di prestare maggiore attenzione alle e-mail ricevute.

Tali mail hanno allegato un file *.one con nomenclatura variabile, sembrano provenire da un determinato account (mentre invece il mittente reale è un altro) e riportano nel corpo della mail un testo generalmente in italiano con riferimenti a possibili conversazioni reali avvenute e carpite in precedenza tramite altre attività malevole. Anche gli oggetti sono tali da indurre nell'utente un senso di sicurezza e spingerlo ad aprire il file allegato e a dare seguito a quanto richiesto nella mail.

Esempi di Oggetto della mail sono: -Fw: Re: RE: Tr: Fwd: RE:[testo di mail recuperato da precedente Leak]

Si tratta di una campagna di phishing a tema EMOTET 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 quanto prima le seguenti azioni nell'ordine riportato:

- Scansione antivirus completa ed approfondita;
- Scansione con software (per esempio AdwCleaner o RogueKiller) per l’individuazione di eventuali Adware, Toolbars, Potentially Unwanted Programs (PUP);
- Pulizia della cache del browser (su Chrome: impostazioni -> "Privacy e Sicurezza" -> "Cancella dati di navigazione" -> Cliccare su "Cancella Dati" per confermare l'operazione);
- Reset e cambio password della casella di posta istituzionale successivamente ai passi sopra menzionati.

Le ricordiamo di prendere visione e di seguire sempre le regole relative le Politiche di Sicurezza adottate dal Ministero raggiungibili nell'apposita sezione dell'area riservata del portale istituzionale https://miur.gov.it.

Cordiali saluti,

CSIRT MIM