- **Oggetto:** CSIRT MI - Raccomandazioni per campagna di malspam Emotet del 29/03/2022
- **Data ricezione email:** 29/03/2022 12:29
- **Mittenti:** noreply@istruzione.it - Gest. doc. - Email: noreply@istruzione.it
- **Indirizzi nel campo email 'A':** <noreply@istruzione.it>
- **Indirizzi nel campo email 'CC':**
- **Indirizzo nel campo 'Rispondi A':** <noreply@istruzione.it>

Allegati

File originale	Bacheca digitale?	Far firmare a	Firmato da	File firmato	File segnato
Mail Emotet di esempio.pdf	SI			NO	NO

Testo email

Gentile Utente,

dall'inizio del conflitto Ucraina Russia si è rilevato un aumento di mail malevole verso le caselle postali istituzionali di MI e Istituti Scolastici.
Il mittente sembra far riferimento a Uffici realmente esistenti all'interno della struttura del Ministero, ma l'indirizzo associato è normalmente sconosciuto e proveniente da domini esteri (per esempio: vinicius.oliveira@kronamaxxi[.]com[.]br, lan.tran.thi.hoa@247post[.]vn oppure valentin.villaseca@automotoraarauco[.]cl). Per inciso gli indirizzi mittenti compaiono senza parentesi quadre.

L'oggetto della mail è variabile e non riproducibile, ma la costante è la presenza di file allegati di diversa nomenclatura con estensione zip contenente al suo interno un file Excel con estensione xlsm. La password per scompattare l'archivio viene messa in risalto.

Si tratta di una campagna di phishing molto aggressiva. Il file Excel allegato alla mail, una volta aperto, lancia una macro che modifica opportunamente il sistema e permette all'attaccante di prendere il controllo della postazione di lavoro, con conseguenze negative non quantificabili su informazioni e dati.

Le chiediamo di non ritenere attendibili tali mail e quindi eliminarle.

Alleghiamo immagine di esempio di una delle mail pervenute a questa Amministrazione per facilitare il riconoscimento della minaccia.

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

Si ringrazia della collaborazione.

CSIRT MI