Da: noreply@istruzione.it
Oggetto: ***IMPORTANTE*** CSIRT MI - EMOTET: Aggiornamento Content Area SIDI ' CSIRT MI'
Data: 30/12/2020 16:41:55

Salve,

la presente per comunicare che nell'area riservata CSIRT MI presente in intranet (sezione: ***Tutti i servizi > Computer Security Incident Response Team****) è disponibile un* ***importante aggiornamento*** *relativo alla* ***campagna di phishing EMOTET*** *- di cui già alle comunicazioni di security awareness dei giorni 22.12.2020 e 29.12.2020 u.s. - in grado di infettare con la sua azione malevola le postazioni di lavoro del personale della Pubblica Amministrazione.*

Nello specifico, si segnalano le nuove caratteristiche delle modalità di attacco informatico:

- *mail mittenti che appaiono 'fidati' anche in risposta (reply) a scambi di email realmente scambiati dall'utente, ovvero a un thread di email in corso;*

- *il cambiamento continuo dell'oggetto mail da una mail malevola all'altra in breve lassi di tempo;*
- *la presenza di allegati in formato compresso per il cui scompattamento si richiede l'inserimento di una password riportata nel corpo dell'email stessa;*
- *dalla possibile presenza di allegati in formato .doc o .xls che dopo essere stati aperti richiedono l'abilitazione per l'avvio di una macro, ovvero l'esecuzione di un'azione che scatena processi interni al computer (l'infezione viene avviata appunto all'atto dell'abilitazione della macro).*

E' fortemente consigliata la lettura dei contenuti di consapevolezza della sicurezza messi a disposizione dallo CSIRT MI, allo scopo di tenersi aggiornati sui rischi informatici incombenti sull'Amministrazione e proteggere sia la propria operatività sia il patrimonio informativo dell'Amministrazione da possibili attacchi.

Grazie della collaborazione

CSIRT MI