Oggetto: CSIRT-MI - Campagna phishing Emotet del 17/05/2022
Mittente: noreply@istruzione.it
Data: 17/05/2022, 16:32
A: noreply@istruzione.it

Gentile Utente,

a seguito di analisi di questo CSIRT, si è rilevato che Lei potrebbe aver ricevuto nella sua casella postale una o più mail con allegato un file *xls oppure un file *zip con all'interno un file *xls con indicata la password necessaria per aprire l'allegato stesso.

La mail sembra provenire da un determinato account (mentre invece il mittente reale è un altro) e riporta nel corpo della mail riferimenti a possibili conversazioni reali avvenute e carpite in precedenza tramite altre attività malevole. Anche gli oggetti sono tali da indurre tranquillamente nell'utente un senso di sicurezza e spingerlo ad aprire il file allegato e a dare seguito a quanto richiesto nella mail. Esempi dell'Oggetto della mail sono:
-Re:, fw:, RE:, FW: Re:[nome mittente]

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);
• 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.

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

L'uso della funzionalità di inoltro automatico è fortemente sconsigliato in quanto rappresenta un rischio sia per la sicurezza dei suoi dati sia di quelli di soggetti terzi, con ripercussioni possibili anche sull'intero patrimonio informativo del Ministero dell'Istruzione, poiché potrebbero essere divulgate o utilizzate da soggetti malintenzionati.

CSIRT MI

Oggetto: CSIRT-MI - Campagna phishing sLoad del 17/05/2022
Mittente: noreply@istruzione.it
Data: 17/05/2022, 17:03
A: noreply@istruzione.it

Gentile Utente,

abbiamo ricevuito segnalazione da parte del Cert Agid che è in atto una campagna di malspam a tema sLoad, solitamente utilizzato per esfiltrare credenziali di accesso a webmail e conti bancari.

Le mail provengono da un indirizzo di posta certificata (PEC) e contengono al loro interno un file .zip, che a sua volta contiene tre file diversi di cui uno .vbs responsabile dell'infezione.

Si fa presente che si stanno individuando le modalità di blocco di tale campagna e che i gestori PEC sono stati avvisati. Si tratta di una campagna di phishing molto aggressiva e 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);
• 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.

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

L'uso della funzionalità di inoltro automatico è fortemente sconsigliato in quanto rappresenta un rischio sia per la sicurezza dei suoi dati sia di quelli di soggetti terzi, con ripercussioni possibili anche sull'intero patrimonio informativo del Ministero dell'Istruzione, poiché potrebbero essere divulgate o utilizzate da soggetti malintenzionati.

CSIRT MI