



Il materiale messo a disposizione nel box denominato "Materiale infettivo da analizzare" è a puro scopo Informativo e di analisi informatica.

Qui di seguito, verrà brevemente descritto quanto disponibile per il download, così da scongiurare qualsiasi problema legato ad un non corretto utilizzo delle risorse.

Carità dal Giappone (Spam)

Si tratta di una mail di spam. Niente di pericoloso durante l'apertura e l'analisi. Si cerca solo ed unicamente di trarre in inganno l'utente finale per cercare di portarlo nel sito web linkato all'interno della mail stessa. Tranquillamente cestinabile.

Rischio: 0/5

Il video della CNN (Virus)

Ci troviamo di fronte ad un caso da poco discusso nei vari forum e siti web dedicati alla divulgazione informatica. Una mail, proveniente da un qualsivoglia indirizzo di posta elettronica (*probabilmente anche conosciuto*) contiene un link ad un "innocuo" file *.asx (*specifico per streaming audio/video in Windows Media Player*). Avviando tale file, Windows lamenterà la mancanza di codec per l'apertura del flusso video. Sarete quindi costretti a scaricare un pacchetto "codec.exe" contenente un virus che, a sua volta, installa svariati malware nella vostra macchina.

Rischio: 3/5 (*dipende dall'attenzione dell'utente*)

Maggiori informazioni sull'articolo sono reperibili all'indirizzo:

<http://www.megalab.it/articoli.php?id=978>

La richiesta dati di Poste Italiane (Phishing)

Il pacchetto, una volta scaricato, contiene due mail da poter aprire/analizzare. Come specificato nella lezione tenutasi durante i primi giorni di corso, ci troviamo di fronte ad un caso di "phishing". Per poter capire meglio da dove arrivano queste mail e, soprattutto, il loro scopo finale, occorrerà analizzare "l'intestazione" (*header*) dove, con un colpo d'occhio, riuscirete a leggere il reale IP/server di partenza della mail.

Lo scopo finale, come sempre, è quello di estorcere – all'utente finale – le credenziali di accesso riguardanti l'istituto bancario "Poste Italiane s.p.a.". Se tali persone dovessero riuscire nell'attacco, avrebbero a disposizione l'accesso completo ai vostri conti, informazioni personali estremamente riservate (*come spiegato nell'apposita lezione*) e, con qualche colpo di fortuna, la possibilità di trasferire il vostro capitale su un loro conto di "appoggio". La seconda mail allegata (*sempre presente nel pacchetto unico*) è un tentativo estremamente mal riuscito. Infatti, noterete che la stessa mail è scritta in un italiano poco comprensibile, tradotto alla buona – molto probabilmente – con un tool apposito reperibile sul web (*vedi google translate o altri*).

Rischio: 4/5 (*dipende dall'attenzione dell'utente*)

Giovanni

www.gfsolone.com – info@gfsolone.com

