C.R.S.T.

C.R.S.T.

12/03/2020

CYBER RISK E CORONAVIRUS

Di Francesca Romana Tubili

I paesi Europei in questo periodo stanno affrontando l'emergenza del Coronavirus. Ma i "virus" sono anche altri. Stanno diffondendosi campagne di phishing e malspam, le quali sfruttano la paura di massa per diffondere pericolosi malware di ogni genere e per carpire dati personali. Come possiamo riconoscere i messaggi di posta elettronica malevoli?

L'allarme è stato lanciato da Sophos, nota azienda di sicurezza informatica, per email che contengono Trickbot in documenti Word, dove si promettono informazioni utili sul coronavirus.

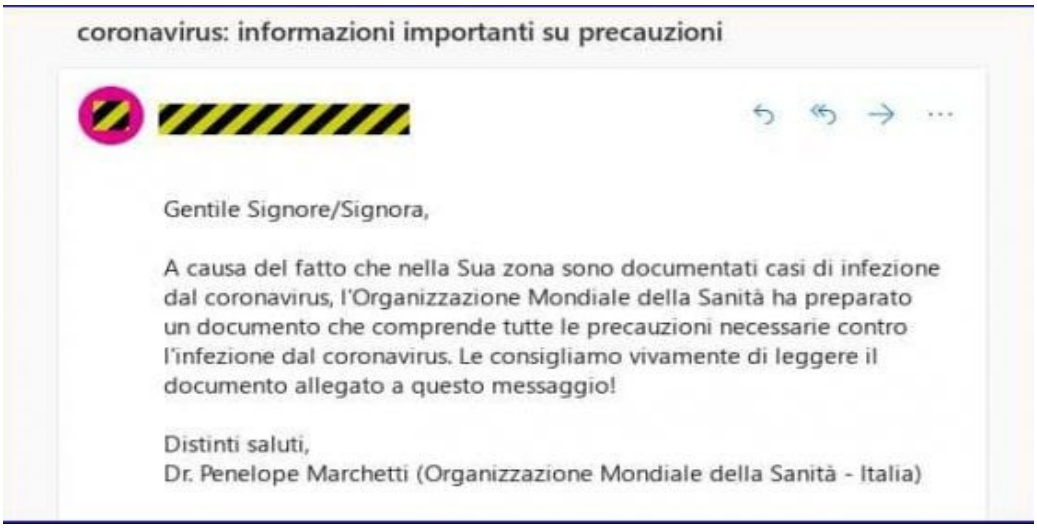
La stessa Polizia di Stato, in merito ad un attacco di phishing ai danni degli utenti delle banche Intesa San Paolo e Monte dei Paschi di Siena, ha diffuso l'allarme. In questo caso, i criminal hacker hanno inviato email con una falsa informativa e una comunicazione urgente in merito all'emergenza sanitaria. L'utente viene indotto a cliccare su un link, il quale lo porta ad accedere all'interno di un portale finto della stessa banca e inserire i suoi dati.

Oltre alla Polizia Postale, anche l'Organizzazione Mondiale della Sanità ha segnalato attacchi di phishing, i quali impersonano l'organizzazione stessa con lo stesso obiettivo: raccogliere dati personali e inoltrare virus per danneggiare i sistemi. In questo caso il messaggio viene inoltrato

direttamente da un funzionario dell'OMS, chiedendo agli interlocutori le proprie credenziali, per poi rimandarli a pagine di destinazione di phishing tramite collegamenti che possono danneggiare i sistemi informatici che vengono utilizzati e gli stessi documenti che sono presenti all'interno.

L'amministratore delegato della Yoroi, Marco Ramilli, spiega che vengono inviate quasi mille email al giorno all'interno delle quali il tema principale è il coronavirus, per rubare i dati personali delle vittime, approfittando della poca prudenza delle persone, le quali cliccano su alcuni link inviati, che promettono delle soluzioni.

Gli esperti dei cyber attacchi consigliano di diffidare delle email che contengono allegati, soprattutto se non attese e di mittenti non noti. Inoltre le banche e l'Organizzazione mondiale della sanità non inviano personalmente email con informazioni utili per contrastare il virus. Per evitare questo tipo di truffa bisogna quindi verificare sempre il mittente, controllando l'indirizzo email, e prestare attenzione quando si forniscono dati personali. Le notizie e le regole da seguire per fronteggiare l'emergenza sono sempre consultabili nei siti ufficiali del Ministero della Salute e della Protezione Civile Nazionale.



Ai cyber criminali inoltre piacciono molto i dati sanitari. Gianvittore Abate, specializzato nel comparto di cybersecurity, in un'intervista al Sole24ore spiega quanto la sanità sia esposta, più

degli altri settori, agli attacchi informatici. Questo perchè, secondo le ultime ricerche Netics, il problema spesso viene sottovalutato; quasi il 20% delle strutture sanitarie non ha la capacità di rispondere velocemente ad un attacco hacker. Gli stessi medici non percepiscono la gravità che possono comportare questi attacchi, per una scarsa conoscenza o attenzione alla materia, per uno insufficiente budget informatico destinato alla sicurezza e per un taglio della spesa fatto dalla Pubblica Amministrazione nel 2018.

Il rapporto Clusit del 2019 ci spiega come la Sanità è diventata il campo più bersagliato, rispetto ad altri settori come banche o industrie, questo perchè si è dimostrata molto proficua. Se il bersaglio è in campo sanitario, il colpo messo a segno da un criminale digitale sale da 150 dollari a 400 dollari.

Il tema sottolinea l'importanza di aumentare la consapevolezza del personale sanitario tramite informazione, formazione e simulazioni di attacchi informatici; incrementare inoltre gli investimenti in cybersecurity e reperire figure specializzate per evitare tempestivamente queste minacce.