PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4937 di Mercoledì 19 maggio 2021

Una panoramica sui messaggi di posta elettronica fraudolenti

Il punto sui 1000 modi in cui un incauto soggetto può trovarsi in gravi difficoltà, non avendo gestito in modo appropriato un messaggio di posta elettronica.

La posta elettronica rappresenta un sistema efficiente ed efficace per truffare il popolo dei navigatori, soprattutto perché non v'è dubbio alcuno che la abilità e fantasia dei malviventi crescano assai più rapidamente, rispetto agli strumenti che un utente può utilizzare per proteggere le sue comunicazioni di posta elettronica.

Ecco il motivo perché ritengo opportuno tracciare di seguito una panoramica sulle varie tipologie di frode, che si appoggiano a messaggi di posta elettronica.

Email spoofing

Con questa espressione si fa riferimento ad un attacco informatico, grazie al quale un malvivente invia un messaggio di posta elettronica, che sembra proveniente da un sito legittimo. L'obiettivo del malvivente è quello di indurre il destinatario ad aprire il messaggio o, peggio ancora, rispondere.

Una forma ancora più pericolosa di questo attacco si manifesta quando all'interno del messaggio di posta elettronica è presente un link, che collega l'incauto navigatore ad un sito, che può scaricare un programma fraudolento nel suo computer.

Phising

Anche questo tipo di attacco rappresenta un metodo per ottenere i dati del navigatore, richiedendo la compilazione di un modulo, che sembra in apparenza inviato da un soggetto legittimo, come ad esempio la Banca, cui il navigatore si appoggia.

Spesso si chiede che questi dati vengano compilati su un modulo, da inviare successivamente ad un indirizzo di posta elettronica, che sembra legittimo, mentre invece è fraudolento. Un occhio attento del navigatore può ad esempio rilevare che l'indirizzo di posta elettronica incorpora delle piccole distorsioni, ad esempio la vocale "o" trasformata in zero, che dovrebbero essere ragione di grave sospetto.

Questo attacco può essere perpetrato perché l'utilizzo di server che usano SMPT ? simple mail transfer protocol-non permette di autenticare l'indirizzo di destinazione.

Domain impersonation

Anche questo tipo di attacco si basa sulla convinzione, da parte del destinatario del messaggio, di essere collegato ad un dominio genuino. Spesso la presenza di errori di battitura, che nascono perché chi invia questi messaggi non ha una buona conoscenza della lingua italiana, rappresenta un indizio significativo.

Spamming

È forse questa la più antica forma di attacco informatico, che consiste nell'inviare una moltitudine di messaggi a decine di migliaia, per non dire milioni di utenti. È bene fare attenzione a che il fenomeno spamming è di per sé un elemento di disturbo, ma non necessariamente comporta che, nel testo del messaggio, siano presenti trappole informatiche di varia natura. Lo spamming, ad esempio, viene utilizzato per propagandare messaggi di tipo politico, senza, appunto, trappole incorporate.

Se poi all'interno del messaggio è inserita una trappola informatica, si ricade in uno degli esempi precedenti.

Come proteggersi

Come accennato, esistono degli applicativi che permettono di proteggere il destinatario di questi messaggi. Ad esempio, il fatto di appoggiarsi ad un gestore di posta elettronica, che offre il servizio a pagamento, piuttosto che gratuitamente, comporta quasi automaticamente l'attivazione di applicativi protettivi, che, ad esempio, mettono in evidenza in caratteri rossi l'indirizzo di un particolare mittente, significando che l'applicativo di protezione ha individuato qualche elemento sospetto.

Tuttavia, di gran lunga più efficace e di più rapida attuazione è la misura di difesa, che si basa su un appropriato addestramento degli utenti. È possibile oggi organizzare dei corsi a distanza, di breve durata, che insegnano agli utenti come riconoscere elementi sospetti nel messaggio, offrendo tutta una serie di esempi di messaggi contraffatti o fraudolenti. Si faccia comunque attenzione che la formazione deve essere di tipo dinamico, perché gli scenari di attacco purtroppo si evolvono assai rapidamente.

Adalberto Biasiotti

---

www.puntosicuro.it