

Il mittente email è davvero chi dice di essere?

L'esercizio vuole mostrare agli utenti alcuni metodi facilmente replicabili per capire se le email che vedono nelle proprie caselle sono legittime o meno. Molti provider email fanno questi controlli a monte e in alcuni casi è molto difficile che messaggi simili finiscano nelle inbox degli utenti. Tuttavia alcuni di questi messaggi possono passare attraverso diversi filtri, e questo esercizio vuole essere uno strumento da utilizzare in questi specifici casi.

Nello specifico analizzeremo il messaggio seguente

CONSEGNA IN ATTESA

Hai (1) pacco in attesa nel nostro magazzino a Parigi pronto per la consegna. Usa il tuo codice per tracciare e ricevere il pacco.

Il tuo numero di tracciamento: 371-346329000

Trova il mio pacchetto

Per chi?

Per utenti dotati di almeno un account email

Durata

Qualche minuto

Livelli arcobaleno + tag/keyword

L3, email, phishing

(secondari)

L0, domini

Difficoltà

Media

Strumenti necessari


- Un account email
- Un client di posta elettronica, può essere sia desktop che web

Costi

0

Istruzioni dettagliate

Alla ricezione di un messaggio email su cui nutriamo sospetti possiamo controllare il mittente in diversi modi. Il primo è di controllare se il dominio (la parte dopo la @) è almeno correlato a chi dice di essere il mittente e che non ci siano errori di battitura al suo interno.

numero di tracciamento: 371-34632900  Posta in arrivo x



Centro di distribuzione <ymubzzegxo@p0ste.it>

 a me ▼

In questo caso sembra che il mittente del messaggio si voglia spacciare per Poste Italiane, utilizzando un dominio molto simile, dove al posto della “O” vi è uno zero.

Se dopo questo controllo abbiamo ancora dei dubbi sulla veridicità o meno del mittente del messaggio, possiamo passare ad un’ispezione più approfondita passando in rassegna le intestazioni (o header) del messaggio. Questa procedura varia da client email a client, però generalmente nelle opzioni disponibili per ciascun messaggio vi è una dicitura che può assomigliare a “mostra originale” (questo su Gmail), “mostra intestazioni” o “mostra dettagli”. Selezionandolo avremo di fronte a noi il corpo del messaggio come è stato ricevuto dal server del nostro provider di posta. Alcuni client (ad esempio Gmail) mettono in evidenza delle informazioni estrapolate, e fra queste vi è l’attributo SPF. L’SPF è un meccanismo per “assicurarci” che il server mittente di quel messaggio sia effettivamente autorizzato a inviare messaggi dal dominio che vediamo dopo la @. Se vediamo, o nelle informazioni in evidenza, o nelle intestazioni una dicitura come “SPF FAIL” possiamo essere quasi certi che il mittente non sia chi dice di essere

A:	nicolo.rebughini@gmail.com
Oggetto:	numero di tracciamento: 371-34632900
SPF:	<u>FAIL</u> con l'IP 185.230.88.247 Ulteriori informazioni

Infine, per concludere il nostro controllo, possiamo analizzare i link all’interno dell’email. Nel corpo dell’email, spostando il cursore del mouse sopra i link cliccabili, possiamo vedere a quali indirizzi essi puntano. Se anche qui vediamo dei nomi strani, per niente riconducibili all’entità che dice di averci inviato la mail o con errori di battitura, possiamo avere una ragionevole certezza di essere di fronte ad un tentativo di phishing.

1imrl7vvyvj9q5pb0j.02.me.uk/rd/r8weksut3h/c25535RCZiZ5358379XudN13831uCS2639vDxd1610

In questo caso infatti i link puntano a nomi i quali sembrano avere solamente lo scopo di confondere l'utente. Se il messaggio fosse legittimo, perchè dovremmo nascondere il servizio di "sblocco pacchi" dietro tutte queste complicazioni?

Risultati attesi

Grazie a questa procedura l'utente dovrebbe essere in grado di ottenere maggiori informazioni per poter formulare delle opinioni informate sulla legittimità di un mittente email.

Lessons learned / Obiettivi

Ci si auspica che in questo modo l'utente, oltre alla sempre necessaria domanda "quello che sto vedendo è legittimo?", abbia degli strumenti in più per costruire anche un processo logico con cui porsi domande aggiuntive per arrivare ad una conclusione più informata.

Prosegui con...

Il dominio del mittente ci può dire parecchie cose. Possiamo proseguire con controlli di tipo "whois" per conoscere l'entità che lo ha registrato: se vediamo che il dominio p0ste.it è stato registrato da un'agenzia di marketing, possiamo farci due domande. Un altro controllo che può tranquillamente decretare la natura di spam/phishing di un'email è un controllo sulle "blocklist": inserendo il dominio in <https://multirbl.valli.org/> e avviando una ricerca possiamo vedere se è già stato segnalato come spam da diversi provider. In più liste un dominio è presente, più alta è la probabilità che sia utilizzato per scopi non legittimi.

Licenza

CC-BY