

Tecnologia

Spam, la spazzatura che intasa sempre più la posta elettronica

Nonostante tutti i filtri il fenomeno sta continuando a crescere

Nella casella di posta elettronica di ciascuno, di solito accessibile attraverso l'interfaccia Web, c'è una cartella spesso ignorata dagli utenti: si chiama «Spam». È lo strumento predisposto dall'azienda fornitrice del servizio per difendere i propri utenti da una piaga della comunicazione moderna: la posta spazzatura. Eppure qualcosa passa sempre. Anche perché il fenomeno è in aumento, come dimostra un rapporto recente pubblicato da Google: in un anno è cresciuto del 6 per cento. E intasa sempre di più la Rete. Perché? A chi giova? E come difendersi, evitando di appesantire ulteriormente il traffico nella Rete?

DI ALESSIO PALMERO APROSIO

Una delle basi fondanti della civiltà moderna, che distingue l'uomo dalla scimmia ammaestrata, è la capacità delle persone di comunicare tra loro in maniera efficiente. Anche migliaia di anni fa una buona rete di comunicazioni poteva ribaltare le sorti di una guerra: già gli Egizi e poi i Romani ne capirono le potenzialità e costruirono un valido sistema per inoltrare le comunicazioni ufficiali e private in tutto il territorio da loro governato. All'alba del Terzo Millennio le comunicazioni si sono evolute fino alla posta elettronica: un sistema semplice, sicuro, efficace e molto economico. Tuttavia queste caratteristiche ne esaltano anche il peggior difetto: l'abuso che se ne può fare.

Carne in scatola

È sfruttando questa potenzialità che nasce il concetto di «spam», traducibile come «posta spazzatura» o «posta indesiderata». Il termine trae ispirazione da un famosissimo sketch del Monty Python's Flying Circus, una serie televisiva trasmessa in Inghilterra a cavallo del 1970, in cui il protagonista finisce in un locale dove servono solamente (e in modo in-

sistente) piatti a base della carne in scatola «Spam». La scenetta, che all'epoca si riferiva a una particolare marca di carne in scatola venduta a prezzi irrisori e quindi diffusissima, rispecchia alla perfezione la frustrazione dell'utente che trova nella propria casella di posta elettronica centinaia di email indesiderate a fronte di qualche decina di messaggi legittimi.

Anche cartaceo, ma non proprio

In realtà lo spam in senso lato può riferirsi anche all'invio di enormi quantità di messaggi non richiesti tramite la posta ordinaria. Si pensi ad esempio alla pubblicità che i centri commerciali, i politici o anche i piccoli imprenditori propongono porta a porta, riempiendo di cartelle le cassette postali. Anche in questo caso sembra di poter parlare di spam. Tuttavia il fenomeno rimane limitato per via degli alti investimenti da parte di chi vuole pubblicizzare prodotti ed eventi. D'altronde proprio il costo elevato fa sì che la pubblicità cartacea veicoli offerte serie e reali: può piacere o non piacere, può essere letta con interesse o cestinata per principio, ma di solito è pubblicità legittima e onesta.

Via email, il fastidio e il pericolo

Un po' diverso è il caso dello spam attraverso l'email. Nella posta elettronica il messaggio si riduce a una semplice connessione tra due computer: quello del mittente e quello del destinatario. Tenendo conto del costo del computer, del costo della connessione a Internet (entrambi ormai alla portata anche del singolo) e del fatto che un computer di media potenza potrebbe spedire centinaia di email al minuto, è comprensibile come l'invio di materiale pubblicitario on line sia un mercato enormemente promettente. Non solo: alla portata anche di malintenzionati, truffatori e cialtroni di varia natura.

Il ragno scandaglia la ragnatela

Tutto il processo inizia con un programma, detto *spider*, che scandaglia la Rete in cerca di indirizzi email nelle pagine Web, nei forum e nelle newsletter. A questi indirizzi lo «spammer», cioè l'autore delle email non autorizzate, aggiunge tutti quelli delle famose e deleterie catene di Sant'Antonio, nelle quali spesso compaiono centinaia di indirizzi



EMAIL
La posta elettronica è un sistema di comunicazione semplice, sicuro, efficace e molto economico. Tuttavia queste caratteristiche ne esaltano anche il peggior difetto: l'abuso che se ne può fare. E sono in molti ad approfittarne. Ma stiamo imparando a difenderci.

in apparenza alla rinfusa. Una volta raccolto un cospicuo numero di indirizzi, lo spammer è pronto per inviare i messaggi.

Battaglia senza fine

L'ultimo rapporto dell'European Network and Information Security Agency (ENISA), pubblicato in gennaio, sostiene che solo il 5 per cento dei messaggi di posta elettronica che viaggiano nella Rete viene consegnato al destinatario. Il restante 95 per cento viene rimosso dai filtri an-

nel 2007, forniva gli stessi risultati. Questo significa che la battaglia senza fine tra i produttori di software antispam e gli spammer che cercano di aggirarli è lungi dall'essere vinta da uno dei due contendenti e rimane sostanzialmente in equilibrio. Se a questo dato si aggiunge che il numero totale di email inviate è in aumento, non stupisce lo studio di Google del 15 aprile, secondo cui il numero di messaggi di posta elettronica indesiderata nel primo trimestre del 2010 è aumentato del 6 per cento rispetto allo stesso periodo dello scorso anno.

La forza dei social network

Nonostante le premesse, però, la guerra allo spam è costellata di tante piccole vittorie che hanno ridotto l'*appeal* e l'importanza della posta spazzatura. I social network, ad esempio, grazie alla loro natura di approvazione dei legami, hanno ridotto moltissimo l'incidenza dello spam. Twitter ha dichiarato nello scorso marzo di aver messo a punto un nuovo filtro che ha drastica-

mente ridotto lo spam all'1 per cento del totale, ben sotto il 95 per cento delle statistiche riguardanti la posta elettronica. Anche Facebook, grazie alle nuove limitazioni sull'invio di messaggi da parte delle applicazioni, ha frenato la diffusione di messaggi indesiderati.

Dentro una campana di vetro

Nonostante questa dovizia di dati e numeri, l'utente finale spesso non è cosciente della tecnologia che protegge la sua casella elettronica da virus, *phishing* e messaggi pubblicitari indesiderati. Infatti i provider cercano continuamente di tutelare la sicurezza dei propri utenti tramite filtri antispam. In questo modo costruiscono una sorta di campana di vetro che abbassa l'attenzione degli utenti esponendoli al rischio di consegnare preziose informazioni nelle mani sbagliate qualora il filtro dovesse risultare inefficace. La morale è sempre la stessa: nella Rete occorre stare sempre all'erta e diffidare sistematicamente dei messaggi che promettono ricchezza, vincite di premi mai richiesti, medicine miracolose, potenziatori sessuali e tutta l'acozzaglia di stupidaggini e truffe che alimentano lo spam.



PUBBLICITÀ, DANNI E TRUFFE

Perché lo fanno? I motivi sono tre

Le principali motivazioni che spingono gli spammer all'invio di email indesiderate sono tre. La spedizione di milioni di email è un ottimo veicolo per pubblicizzare prodotti quando i canali istituzionali non sono molto adatti oppure esistono norme che ne rendono illegale la vendita. Inoltre la pratica dell'invio massiccio di messaggi a destinatari non consenzienti è illecita in molti Paesi: difficilmente un'azienda tradizionale e onesta ne fa uso. Per questo motivo piombano spesso nelle caselle di posta elettronica gli inviti di avvenenti fanciulle dell'Europa orientale oppure suggerimenti per procurarsi Viagra e Valium a prezzi allettanti. In seconda battuta, la posta elettronica è il veicolo prediletto dai programmatori malintenzionati per diffondere virus, ossia programmi informatici che, una volta eseguiti dal computer, causano danni di vario tipo: invio di informazioni riservate, cancellazio-

ne di file, utilizzo del computer della vittima come base per connessioni illecite in modo da risultare difficilmente rintracciabili. Spesso inoltre il virus, una volta installato, sfrutta nuovamente la posta elettronica per autoinviarsi a tutti i contatti presenti sul computer e sperare che qualche altro malcapitato abbocchi e apra l'email. Negli ultimi anni, infine, una nuova piaga causata dallo spam ha cominciato ad affliggere Internet: il fenomeno del *phishing*. La vittima riceve un messaggio di posta elettronica, in apparenza inviato dalla propria banca, in cui viene invitato a seguire un link e a inserire le credenziali del proprio conto corrente, pena la perdita di un'ingente somma di denaro oppure la chiusura del conto stesso. L'utente viene trasferito su un sito Web esteriormente identico a quello della banca ma in realtà fasullo, e lì invitato a fornire i suoi dati di autenticazione. Dietro

quella pagina si trova ovviamente un truffatore che poi si appropria del conto corrente della vittima per effettuare un cospicuo bonifico in un paradiso fiscale. Nonostante la massiccia attività delle banche per contenere il problema, decine di persone cadono ogni giorno in questi tranelli, rischiando di vedersi svuotato il portafoglio virtuale.

PROGRAMMI DI DIFESA, LISTE NERE E STRATAGEMMI

Le contromisure di utenti e provider

Per riuscire a combattere la piaga dello spam esistono programmi appositi, detti filtri antispam. Secondo l'ultimo rapporto dell'ENISA, pubblicato in gennaio, un terzo dei grossi provider destina più di un milione di dollari annui in questo settore. Il funzionamento dei filtri antispam è piuttosto semplice. A ogni messaggio di posta elettro-

nica viene assegnato un valore numerico: più il valore è basso, più il messaggio è affidabile. Superata una soglia predeterminata, il messaggio è considerato spam e cestinato. I parametri che determinano questo valore dipendono da alcuni fattori: le parole chiave contenute nel messaggio, la sua provenienza, la lingua in cui è scritto. Inoltre, grazie all'appoggio di provider e gestori di posta elettronica, sono state stilate a livello internazionale alcune liste di server inaffidabili (dette *blacklist*), dalle quali diventa semplice rigettare la posta elettronica. Anche nel nostro piccolo universo di utenti singoli possiamo adottare alcune misure per prevenire la ricezione di posta elettronica indesiderata. Bisognerebbe ad esempio evitare di indicare il proprio indirizzo di posta elettronica nei forum, nei commenti ai blog, nelle newsletter. Alcuni utenti usano strata-

gemmi che ingannano gli spider, ma non l'allenato occhio umano. L'indirizzo «utente@dominio.ch» potrebbe diventare «utenteTOGLIMI@dominio.ch» oppure «utente@dominio.punto.ch». È opportuno anche evitare di rispondere alle catene di Sant'Antonio inserendo gli indirizzi nei campi «A» o «Cc». Per inoltrare un messaggio di posta elettronica a molti destinatari, è più sicuro utilizzare il campo «Ccn» («Bcc» in inglese), attraverso il quale i singoli destinatari non possono risalire all'elenco completo. Nel caso di ricezione di email palesemente indesiderate, è bene evitare di cliccare sui collegamenti del tipo «Clicca qui se non vuoi più ricevere questi messaggi», perché di solito sono armi a doppio taglio che regalano ai malintenzionati l'informazione che l'indirizzo email da cui è partita la richiesta esiste ed è regolarmente consultato.

