

QUANDO LA POSTA VA RIPULITA

Stefano Zanero, CTO e fondatore, Secure Network S.r.l.

Davide Veneziano, Security Consultant, Secure Network S.r.l.

Chiunque utilizzi la posta elettronica si trova sempre più frequentemente di fronte a messaggi-spazzatura non richiesti; un vero e proprio diluvio, in continuo aumento. Secondo recenti statistiche, si valuta che addirittura una percentuale oscillante tra il 50 ed il 55 per cento del numero totale delle e-mail circolanti su Internet siano da considerarsi "spam". E la percentuale è in continua crescita.

Molto dipende anche dalle definizioni che diamo di "spam". In questo articolo, parleremo in generale di tutti quei messaggi non richiesti che infastidiscono chi li riceve. Possiamo tuttavia fare una macrodistinzione tra:

- UCE (Unsolicited Commercial E-mail): rappresentato da tutti quei messaggi commerciali caratterizzati da diffusione massiccia, rappresenta la più ampia parte dello spam
- UBE (Unsolicited Bulk E-mail): messaggi a diffusione massiccia che, a differenza dell'UCE, non sono a carattere commerciale. In questa categoria rientrano ad esempio le catene di S.Antonio, le richieste di aiuto, i worm e le truffe.

La lotta allo spam è cominciata da tempo, ma gli spammer si sono sempre dimostrati sempre molto versatili e competenti, avvelendosi delle risorse più convenienti messe inavvertitamente a loro disposizione fino ad ottenere dei costi di invio praticamente nulli. Se inizialmente si sono serviti di relay e proxy aperti o mal configurati, al giorno d'oggi la tecnica più usata è lo sfruttamento di macchine di utenze private dotate di connessione a banda larga e compromesse da trojan o worm. Questo dimostra anche come il legame tra spammer e virus writer sia sempre più forte.

Tutto ciò ha costretto i principali provider a correre ai ripari. Al giorno d'oggi, l'unica strategia applicabile è il filtraggio in ricezione, ovvero prima che il messaggio di posta giunga nella casella dell'utente. Agendo al livello del server di posta, l'amministratore di sistema si può avvalere principalmente di due metodologie di filtraggio.

L'utilizzo di blacklists e blocking lists (DNSBL) rappresenta un metodo veloce ed efficace di contenimento. Difatti, attraverso una semplice richiesta DNS, il server mail ricevente è in grado di verificare se l'indirizzo IP mittente sia presente nelle liste. In caso affermativo potrebbe decidere di troncatura la comunicazione: in questo modo non si ottiene soltanto una benefica riduzione di spaq per gli utenti, ma anche un forte risparmio in termini di banda, storage e risorse, in quanto interrompendo direttamente la transazione SMTP non è richiesta la ricezione completa della e-mail. Tuttavia, c'è il problema di scegliere quali liste utilizzare, e questo è un compito arduo che richiede preparazione, impegno e attenzione continua, dato che l'amministratore dovrà scegliere quelle adatte a modellare le esigenze proprie e dell'utenza in modo da evitare la perdita di posta legittima.

Il Content Filtering, ossia il filtraggio basato sul corpo del messaggio, rappresenta un'altra tecnica di contenimento in forte diffusione. In questo caso tuttavia il messaggio deve essere completamente ricevuto dal server affinché il filtro possa agire con efficacia. In questo caso dunque non abbiamo risparmio di banda, e il filtro stesso consuma risorse computazionali. Tuttavia, il vantaggio è quello di avere a disposizione maggiori informazioni su cui basare la valutazione; inoltre l'uso di filtri statistici e di sistemi di apprendimento (come ad esempio i famosi filtri bayesiani) rappresenta un ulteriore strumento in grado di facilitare la classificazione tra un messaggio di posta legittimo e uno di spam, anche sulla base della percezione dell'utente e non soltanto di una classificazione a priori tra IP buoni e cattivi.

Queste due filosofie sono complementari, e la nostra esperienza ci indica come il loro utilizzo congiunto porti al migliore risultato e alla massima efficacia. Tuttavia, una certa dose di competenza

e di attenzione continua è necessaria per ottenere buoni risultati di rilevamento e bassi tassi di falsi positivi.

Se questi metodi sono, ad oggi, l'unico aiuto contro il dilagare dello spam, non sono certo una soluzione a lungo termine. Tuttavia, al giorno d'oggi non si vede all'orizzonte nessuna soluzione definitiva, anche se molte proposte sono state avanzate per ovviare al problema. Una proposta ricorrente è ad esempio la ridefinizione del protocollo di posta, superando SMTP che è carente riguardo ai requisiti di sicurezza ed identificazione. Lavora al progetto il gruppo MARID della Internet Engineering Task Force (IETF).

Un'altra interessante proposta si basa sul concetto di "identificazione del mittente". Con questo meccanismo, ogni provider dichiara da quali indirizzi IP è lecito aspettarsi posta avente il proprio dominio come mittente. Si stima che tra il 50 e il 70 per cento dello spam totale potrebbe essere bloccato utilizzando questa metodologia tutto sommato semplice. Esistono numerose proposte per l'implementazione pratica di questa filosofia, la più supportata attualmente è il Sender Policy Framework (SPF <http://spf.pobox.com>), proposto in origine da AOL e adottato al giorno d'oggi già da diversi provider. Anche in questo caso le informazioni possono essere distribuite tramite l'architettura DNS, e i principali server SMTP possono adattati per utilizzare questo metodo. Altre proposte analoghe sono state Domain Keys di Yahoo e Caller-ID di Microsoft (www.microsoft.com/spam). Tutte queste proposte, tuttavia, necessitano una forte diffusione del metodo in questione per poter divenire veramente efficaci e per questo al giorno d'oggi non rappresentano un metodo sufficientemente efficace per combattere lo spam.

Un'altra proposta, la più recente, è stata portata da Spamhaus (www.spamhaus.org), un organismo che partecipa attivamente alla lotta contro lo spam da molti anni. Si tratta dell'istituzione di un TLD .mail che rappresenti una "lista" di provider "buoni", che non supportano gli spammer (www.spamhaus.org/tld). La proposta è già stata inoltrata ad ICANN, e solo il tempo dirà se avrà successo davvero.

Va anche ricordato che sia la legislazione europea sia quella americana si sono preoccupate di elaborare norme ben precise per cercare di arginare il fenomeno. L'Italia, seguendo le direttive europee, ha inserito tali norme nel D. Lgs. 196/03, noto come "Testo Unico sulla Privacy". Viene imposto il divieto assoluto di inviare qualsiasi genere di comunicazione pubblicitaria senza il preventivo consenso dell'interessato (art. 130, comma 1), definendo quindi una politica detta di tipo "opt-in". Inoltre, l'articolo 130 comma 5 vieta in ogni caso di utilizzare un mittente non identificabile o irraggiungibile per le comunicazioni di questo tipo, prevedendo una forte sanzione pecuniaria in caso di violazione. La legislazione italiana attribuisce inoltre al Garante della Privacy il potere di sanzionare gli spammer italiani (art. 130 comma 6).

Anche la nuova legge degli USA (detta provocatoriamente "CAN-SPAM act") punisce l'invio di mail con mittente contraffatto (con pene che arrivano al carcere) rappresenti complessivamente un forte passo indietro nei confronti della lotta allo spam dato che, contrariamente a quanto avvenuto in Europa, viene accettata una politica di tipo "opt-out", che rende in pratica legale lo spam, vincolandolo alla sola presenza di un metodo che consenta di disiscriversi dalla lista e non ricevere ulteriori comunicazioni.

Tuttavia va considerato il limite intrinseco di queste soluzioni di tipo normativo: anche se indubbiamente positive, le leggi contro lo spam vengono adottate da un singolo stato e valgono entro i suoi confini nazionali. Questo non è sufficiente a sconfiggere un fenomeno di natura assolutamente transnazionale.

Secure Network S.r.l. (www.securenetwork.it) è una società di consulenza, formazione e servizi alle imprese focalizzata sui temi della sicurezza informatica.

BOX: SE I VIRUS SI MESCOLANO ALLO SPAM

Ormai ogni virus su Internet è “da record”. Milioni di macchine vengono compromesse a causa di vulnerabilità per cui esistono da tempo le opportune patch, o a volte senza nemmeno bisogno di vulnerabilità, col sempreverde metodo dell’allegato eseguibile. E se avevamo qualche illusione su quanto fossero ascoltati i consigli in proposito, ce le ha tolte il virus Novarg, che arrivava come file compresso. Le persone aprivano il file zip ed eseguivano il contenuto, con una concentrazione suicida da far invidia a un lemming.

Il problema tuttavia è ampio e complesso, e la risposta ancora non l’abbiamo trovata. La rincorsa degli antivirus continua da 20 anni, ed ormai abbiamo il legittimo sospetto che sia come la corsa di Achille e della tartaruga nel famoso paradosso: firme sempre più rapide, aggiornamenti sempre più frequenti... e i virus sono sempre qualche metro avanti, qualche ora avanti, a volte qualche minuto avanti. Abbiamo messo scanner antivirus sui client, sui server, sul mailserver, li stiamo integrando anche nei firewall. Ed ancora i virus passano, e devastano. Non solo, ma dopo aver devastato la nostra rete ne escono, rendendoci “corresponsabili” di ulteriori infezioni; inoltre, le macchine compromesse spesso hanno delle backdoor pronte per trasformarle in “macchine da spam”.

Se gli antivirus sono solo un palliativo, forse anche per i worm via posta elettronica una possibile risposta definitiva sta nell’evoluzione di un nuovo protocollo di posta che autentichi i server autorizzati, evitando il mass mailing da postazioni client.