

Spamming: perché infastidisce e come combatterlo

La parola *spam* deriva dalla contrazione dei termini “*spiced ham*”, e negli U.S.A. è il nome dato ad una nota marca di carne di maiale in scatola. Ma come mai, oggi, lo stesso termine indica un fenomeno che coinvolge la comunità Internet? Il tutto ha inizio da uno sketch televisivo in cui, in un ristorante, mentre una coppia cerca di ordinare la propria cena, un gruppo al tavolo vicino copre le loro voci urlando con insistenza la parola *spam*¹. La coppia è irritata da questo atteggiamento, così come oggi molti utenti della rete sono irritati dalla enorme quantità di messaggi spazzatura che invadono la loro casella di posta elettronica. *Spam* è, dunque, sinonimo di “disturbo della comunicazione”, realizzato solitamente attraverso un insieme di messaggi indesiderati che presentano carattere di molteplicità e ripetitività, e che sono stati spediti senza il consenso preventivo del destinatario^{2, 3}.

Secondo i più recenti studi condotti dalla società IDC, entro il 2005 oltre il 40% dei messaggi di posta elettronica scambiati sulla rete sarà costituito da *spam*, un dato piuttosto allarmante, soprattutto alla luce del potenziale danno che questo fenomeno causa alle aziende. Basti pensare alla riduzione di produttività del personale (tempo speso per il download e la lettura dei messaggi, tendenza dell’utente a dare meno credito ai messaggi di posta elettronica), all’aumentato costo delle risorse IT (pensiamo al costo “in banda” di elaborazione e download dei messaggi, al costo di memorizzazione dei messaggi – investimenti in strumenti di storage e backup – al lavoro addizionale per lo staff IT), ai rischi legali (coinvolgimento/responsabilità legale dell’azienda) e infine, alla diminuzione della sicurezza globale sulla rete (i messaggi sono sovente ingannevoli o portatori di codice malevolo e virus). Lo *spam* si configura, quindi, sempre più come una sorta di furto di servizi, e si traduce in una sostanziale perdita finanziaria per le aziende. Per queste ragioni è arrivato a rappresentare un problema molto sentito anche in ambito europeo, al punto da spingere numerose nazioni dell’Unione a criminalizzare il fenomeno e a premere per la definizione di una legislazione chiara in materia (si pensi all’istituzione del comitato EuroCAUCE, sulla scia dell’omologo americano CAUCE, ed alla volontà di approvare in tutta l’Unione una normativa basata sul consenso preliminare – OPT-IN⁴).

Oltre agli aspetti normativi, che rivestono un ruolo essenziale nella tutela dell’utenza, notevole importanza in questo ambito ha la tecnologia, grazie alla quale si può contrastare efficacemente il fenomeno e ridurre in maniera significativa la perdita finanziaria indotta dallo spamming. Molte sono le aziende che offrono sul mercato prodotti antispam specifici (citiamo ad esempio Trend Micro e Nokia) o che hanno incluso un motore antispam nei propri sistemi (pensiamo all’esempio di Fortinet che sta per introdurre funzionalità antispam a bordo dei propri antivirus firewall della linea Fortigate⁵). La maggior parte dei vendor realizza sistemi in grado di effettuare controlli combinati su più fronti, che prendono in esame sia il livello di trasporto dei messaggi, sia i contenuti dei medesimi. In altre parole, i meccanismi più moderni – noti con il nome di *motori cocktail* - si basano su una combinazione di più tecniche che vanno dal tradizionale impiego delle black list usate per isolare un noto insieme di domini di posta “generatori” di spam, all’analisi testuale del corpo e/o dell’oggetto del messaggio alla ricerca di termini sospetti, all’esame delle immagini contenute nel corpo del messaggio, sino all’analisi euristica dei messaggi in arrivo (es. Trend Micro Spam Prevention Service, Nokia Message Protector⁶), ed ancora ai più complessi filtri bayesiani, che operano sull’intero

¹ <http://www.detritus.org/spam/skit.html>

² <http://www.colinelli.net/antispam>

³ <http://spam.abuse.net>

⁴ <http://spamlaws.com/eu.html> ; <http://www.euro.cauce.org/it/>

⁵ <http://www.fortinet.com/products/>

⁶ <http://it.trendmicro-europe.com/enterprise/products/groups.php?prodgroup=1&family=27> ; http://www.nokia.com/networks/product_catalog/pc_product_highlights/1,6929,,00.html?prod_id=NIC00031&path=mca&t&mcat=138263&scat=134843

messaggio di posta cercando di determinare la probabilità che il messaggio sia *spam* e sfruttando poi i risultati del processo di riconoscimento per le fasi decisionali successive (auto-apprendimento). La combinazione di più metodologie di analisi, e soprattutto l'impiego di tecniche dinamiche, consente ormai di raggiungere elevati valori di efficacia (*capture rate*), al punto da arrivare spesso ad identificare il 90-95% dei messaggi *spam*⁷.

Va osservato però, che la scelta di un prodotto anche di ottimo livello, da sola, non sempre permette di garantire risultati efficaci. Un detto di Sun Tzu, tratto dalla sua celebre opera "L'arte della guerra", recita: "E' un vantaggio poter scegliere il tempo ed il luogo della battaglia". E' molto importante, infatti, stabilire la strategia di difesa che si intende adottare, perché la stessa condiziona sia la scelta del prodotto più idoneo al contesto, sia il disegno architetturale del sistema antispam, sia la configurazione dei sistemi di posta elettronica con i quali la soluzione antispam si deve integrare. In generale, se ci riferiamo alla collocazione dello strumento⁸, possiamo catalogare le soluzioni antispam in:

- soluzioni desktop, realizzate mediante software collocato direttamente sulla stazione utente;
- mail server plug-in, basate su software da collocare sul mail server interno dell'azienda (es. Trend Micro Scan Mail e-Manager);
- mail relay plug-in, basate su software da collocare sul "message transfert agent" dell'azienda (es. es. Trend Micro InterScan e-Manager);
- e-mail firewall, costituite da strumenti dedicati posti in corrispondenza del perimetro della rete (es. Nokia Message Protector, Trend Micro Spam Prevention Service).

La scelta della soluzione va fatta sia nell'ottica di contrastare efficacemente le problematiche aziendali richiamate in apertura (Tabella 1), sia in funzione di altri elementi, come la fruibilità per l'utenza ed il livello di controllo globale che lo staff IT può esercitare sul sistema (Tabella 2).

	Desktop	E-Mail Server plug-in	MTA plug-in	E-Mail firewall
Produttività	-	+	+	+
Risorse IT	--	-	-	+
Rischi Legali	--	+	+	+
Sicurezza	-	+	+	+
	--	+	+	+++

Tabella 1

	Desktop	E-Mail Server plug-in	MTA plug-in	E-Mail firewall
Efficacia (<i>capture rate</i>)	+	+	+	+
Funzionalità supplementari	--	-	-	+
Gestione	--	-	-	+
	--	-	-	+++

Tabella 2

In generale, l'utilità e la convenienza della soluzione crescono al crescere del livello di accentramento dei controlli – come è possibile verificare anche dall'esame delle tabelle – sia perché si ottiene un miglior controllo del sistema e si sgrava l'utenza dall'onere di dover gestire ulteriori strumenti di protezione, sia perché la disponibilità di un sistema dedicato evita l'appesantimento di altri sistemi e risorse (ad esempio, un mail server che debba operare anche un'analisi antispam mediante e-mail plug-in, diverrebbe potenziale vittima di attacchi *Denial of Service* in tutti i casi in cui la mole di messaggi da gestire dovesse superare una soglia critica).

Nonostante l'attuazione di contromisure sempre più sofisticate, va detto che lo spam continua a rappresentare un fenomeno consistente, ed anzi in crescita, soprattutto nell'ultimo anno. Tuttavia, l'intensificarsi della battaglia contro questo malcostume, tanto sul fronte legale quanto su quello della

⁷ <http://spamconference.org/proceedings2003.html>

⁸ Tumbleweed Communications – Architectural comparison of enterprise antispam solutions – 2003 ; <http://www.sans.org/rr/papers/index.php?id=870>

tecnologia, e la crescita di consapevolezza da parte di aziende e singoli fa sperare che presto o tardi ciascuno possa decidere di ricevere nella propria casella di posta elettronica solo ciò che gli interessa effettivamente.