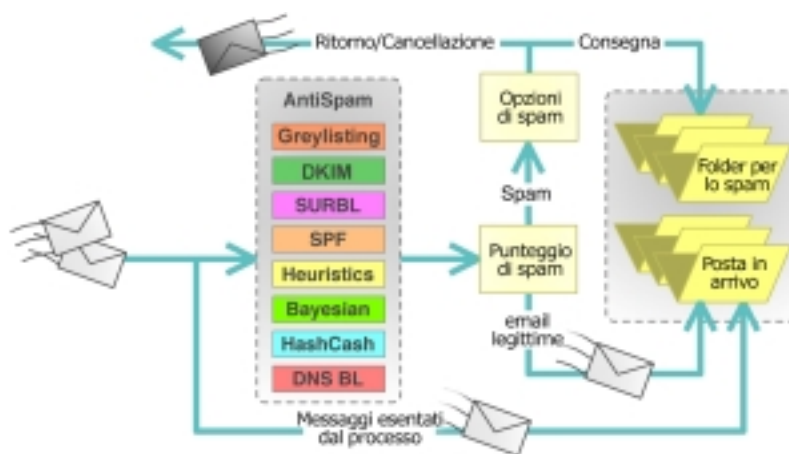


MDaemon contro lo spam

Oltre il 50% del volume di posta elettronica che circola in Internet è costituito da spam, ovvero messaggi non richiesti e non graditi. Vera e propria piaga della Rete, lo spam consuma inutilmente la banda e rallenta il recapito delle email legittime. Tuttavia, anche quei pochi destinatari che rispondono a questi messaggi non richiesti sono sufficienti a rendere lo spam un'attività proficua.

Lo spam rappresenta un serio problema in termini di spreco di banda, di capacità di elaborazione e di spazio su disco. Se non viene tenuto sotto controllo, lo **spam divora tempo prezioso** per controllare e scartare i messaggi non desiderati.

Per evitare lo spreco di risorse causato da questi messaggi non richiesti MDAemon mette a disposizione diversi strumenti AntiSpam. Sebbene non esista un singolo metodo per fermare lo spam, l'azione combinata delle diverse tecniche AntiSpam presenti in MDAemon consente di attenuare sensibilmente il problema.



Combattere lo spam senza perdere messaggi

Impostazioni AntiSpam efficaci

La mente umana è nettamente superiore al miglior filtro antispam. Normalmente riconosciamo lo spam già dal nome del mittente o dall'oggetto del messaggio. Sebbene la tecnologia per combattere lo spam non possa raggiungere il livello di precisione della nostra mente, l'AntiSpam di MDAemon riesce comunque ad andarci assai vicino.

Utilizzando le impostazioni predefinite, gli stru-

menti AntiSpam individuano infatti dall' 80% al 95% dello spam senza falsi positivi.

Quindi, **anche un utente alle prime armi può attivare l'AntiSpam di MDAemon** senza timore di perdere messaggi importanti.

Gli strumenti AntiSpam di MDAemon mettono a disposizione dei più esperti numerose opzioni per una configurazione avanzata aiutando a individuare, evidenziare, mettere in quarantena ed eliminare lo spam.

Motivazioni economiche dello spam

Lo spam esiste perché anche una minima percentuale dei milioni di destinatari bersagliati quotidianamente dagli spammer risponde ai messaggi acquistando i prodotti o i servizi reclamizzati. Un altro vantaggio economico per gli spammer è legato al fatto che l'invio di grandi volumi di email non costa quasi nulla: sono infatti le aziende che usano Internet e le persone che ricevono email non richieste a sopportare i costi dello spam.

Come operano gli spammer

Gli spammer spediscono i messaggi attraverso email server SMTP, proprio come fanno tutti quelli che usano la posta elettronica. Tuttavia, per inviare spam occorre seguire alcuni accorgimenti per sfuggire ai controlli: cambiare di sovente i server, servirsi di diversi Internet provider, installare server locali, ricorrere a server open relay su Internet, avvalersi di servizi email gratuiti e sfruttare computer altrui controllati mediante tecniche pirata. Non è quindi semplice bloccare uno spammer.

Analisi dei messaggi e attribuzione dei punteggi di spam

L'AntiSpam di MDAemon assegna un punteggio a ogni messaggio in ingresso. Ciascuno strumento AntiSpam può aggiungere o togliere punti al messaggio. Nel momento in cui il punteggio raggiunge la soglia impostata, l'AntiSpam etichetta il messaggio come spam.

Quando un messaggio viene riconosciuto come spam può dunque essere rispedito al mittente, cancellato, inoltrato a una cartella pubblica creata per archiviare lo spam, oppure normalmente processato dalle tecniche di filtraggio dei contenuti ed eventualmente recapitato al destinatario.

Il filtro per i contenuti può intervenire in modi diversi sui messaggi spam, ad esempio aggiungendo un apposito avviso nell'oggetto dell'email. Per gli utenti che usano IMAP e WorldClient, lo spam può essere smistato automaticamente in appositi folder.

Greylisting

Greylisting è una tecnica innovativa per fronteggiare lo spam che si basa su un piccolo trucco: **rifiutare temporaneamente tutti i messaggi ricevuti**, siano essi legittimi o indesiderati.

Se dotato di capacità di greylisting, il mail server che riceve l'email rifiuta ogni messaggio ricevuto per un periodo di tempo arbitrario, restituendo un codice di "errore temporaneo". In questo caso il server mittente prova nuovamente a consegnare il messaggio; **scaduto il tempo di rifiuto** da parte del server destinatario il tentativo andrà a buon fine e **il messaggio sarà accettato e quindi consegnato**.

Solo i mail server legittimi provano a rispettare i messaggi. I mail server utilizzati dagli spammer non possono permettersi il lusso di riprovare semplicemente perché devono inviare milioni di messaggi.

Il greylisting può causare effetti indesiderati: respingere la prima volta ogni messaggio significa infatti rallentare la consegna della posta. Per mitigare questi problemi MDAemon mette a disposizione una serie di opzioni che permettono di utilizzare la tecnica del greylisting con inconvenienti minimi. Per esempio, si può configurare il mail server in modo che rifiuti solo il primo messaggio di un determinato mittente; tutti i messaggi successivi provenienti dal medesimo indirizzo verranno immediatamente accettati e consegnati.

DNS Black List

Uno dei principali metodi di identificazione dello spam consiste nel **confrontare l'indirizzo del mittente con gli indirizzi contenuti all'interno di black list** di libera consultazione che elencano gli spammer e i server open relay conosciuti.

Un server open relay è un server che consente l'invio di email da qualunque mittente a qualunque destinatario senza effettuare controlli.

Queste liste, note anche come "DNS Black List", sono disponibili su diversi siti Web e contengono gli indirizzi IP dei mail server che effettuano spam. Il DNS black listing (il mecca-

nismo di verifica delle black list) confronta gli indirizzi dei server da cui provengono i messaggi con quelli contenuti nelle black list. Se coincidono, i messaggi vengono etichettati come possibile spam aumentando il punteggio ad essi associato.

Ciascuna lista è gestita secondo criteri arbitrari per quanto attiene all'aggiunta o alla rimozione dei mail server dall'elenco. Le black list utilizzate da MDAemon hanno dato, nel tempo, prova di affidabilità.

Rilevare i siti Web che supportano lo spam

Gli spammer che sfruttano il Web per vendere i propri prodotti cambiano spesso gli indirizzi di posta elettronica; raramente, invece, cambiano i siti Web usati come negozio. Una nuova tecnologia anti-spam trae vantaggio proprio da queste peculiarità per individuare lo spam.

Si tratta della tecnologia SURBL, o Spam URI Realtime Blocklists. SURBL, implementata in MDAemon, **ricerca nei messaggi in ingresso alcuni identificatori detti URI** (Uniform Resource Identifiers) e **li confronta con una lista di indirizzi Internet** noti per la loro complicità con gli spammer.

Quando un indirizzo Web contenuto nel testo di un'email è associato a uno di questi siti, MDAemon etichetta il messaggio come possibile spam.

Chi si avvale di tecnologia SURBL apprezza, usando unicamente questo strumento, una riduzione dello spam che arriva al 60%.

Rilevare le false identità

Il termine inglese *spoofing* indica l'uso non autorizzato o la contraffazione di un indirizzo email o di un nome di dominio. Questa tattica consente al mittente di nascondere la propria identità.

Gli spammer si avvalgono spesso dello ***spoofing* per nascondersi dietro al nome e all'indirizzo email di altre persone** e invogliare i destinatari ad aprire i loro messaggi e a rispondere.

Uno degli utilizzi più pericolosi dello *spoofing* è il *phishing*: una tecnica che permette di ge-

nerare **messaggi che fingono di provenire da fonti sicure e autorevoli** come servizi di pagamento online, banche e ISP. Questi messaggi, spediti da spammer che si avvalgono di identità contraffatte, chiedono al destinatario di aggiornare o confermare i propri dati personali o il numero della carta di credito via email, oppure attraverso siti Web dall'aspetto ufficiale, ma in realtà del tutto fasulli.

MDaemon si avvale di uno strumento denominato *SPF/Sender-ID* (*Sender Policy Framework*) per smascherare gli indirizzi email impropriamente utilizzati. **SPF/Sender-ID è una tecnica di sicurezza per convalidare gli indirizzi dei mittenti.** Quando un indirizzo email risulta essere contraffatto, il messaggio può essere etichettato come probabile spam.

DomainKeys Identified Mail - DKIM

Un'altra tecnologia in grado di impedire agli spammer di dissimulare la loro identità è denominata DomainKeys Identified Mail. DKIM aiuta a combattere il *phishing*.

Il principio su cui si basa DKIM è quello di **integrare nei messaggi inviati una firma digitale crittografata** accoppiata a una firma sul server che invia il messaggio. Il server del destinatario verifica la firma dei messaggi in ingresso e blocca quelli la cui firma non corrisponde a quella del server mittente.

DomainKeys Identified Mail è un nuovo standard supportato da numerose grandi aziende del settore. **MDaemon è il primo mail server Windows a supportare questo nuovo standard.** Alt-N ha svolto un ruolo attivo all'interno del comitato tecnico che ha definito lo standard DKIM.

Controllare i messaggi confrontandoli con modelli

MDAemon si avvale della **tecnologia euristica** di SpamAssassin per identificare i messaggi non richiesti. Questa tecnologia **analizza i messaggi attraverso regole basate su modelli** costruiti analizzando milioni di esemplari di spam. Le regole fanno riferimento a diverse parti di un'email come l'indirizzo del server da cui è stata inviata, il mittente, l'oggetto del messaggio e il corpo ve-

ro e proprio. Per esempio, un messaggio che contenga testo HTML di colore rosso e un link potrebbe essere riconosciuto come spam non tanto per il contenuto in sé quanto per le caratteristiche di formattazione del messaggio stesso.

Il confronto di tipo euristico prevede l'applicazione di tutte le regole a ciascun messaggio. **Ogni qualvolta un messaggio soddisfa la regola, l'email riceve un punteggio** che ne indica la potenziale natura di spam. Quando il punteggio raggiunge la soglia impostata, MDAemon può etichettare il messaggio come probabile spam.

Negli ultimi anni la tecnologia euristica è diventata molto affidabile nel rilevare lo spam e MDAemon aggiorna costantemente le proprie regole euristiche in accordo con le più recenti novità fornite da SpamAssassin.

Lo spam: una definizione

Il rilevamento dello spam è ancora più accurato se la tecnologia AntiSpam riesce a riconoscere la differenza tra email legittime e email indesiderate per ogni singolo mail server o per ogni singola azienda. All'interno di MDAemon questo compito è affidato a **tecniche di classificazione bayesiana**.

La classificazione bayesiana funziona analizzando campioni di entrambi i tipi di messaggio: spam e non-spam. Amministratori e utenti autorizzati forniscono al software bayesiano esempi concreti di email legittime e email indesiderate.

Lo strumento bayesiano analizza l'intero contenuto di ogni esempio e confronta con queste informazioni tutti i messaggi in ingresso.

Aggiungendo quotidianamente degli esempi, la classificazione bayesiana diventa sempre più precisa e può raggiungere il 90% di accuratezza con un margine quasi nullo per quanto riguarda l'errata identificazione delle email lecite (falsi positivi).

Configurando opportunamente MDAemon, si possono aggiungere esempi di email legittime attraverso processi completamente automatici.

Black List, White List, e liste di esclusione locali

Le funzioni di MDAemon per combattere lo spam si avvalgono anche di black list, white list ed eccezioni, gestite localmente.

I messaggi destinati a indirizzi contenuti nella white list sono esentati dalle verifiche inerenti le DNS Black list.

Per il filtro AntiSpam **la presenza di un indirizzo in una black list significa che da quell'indirizzo è possibile che arrivino dei messaggi di spam**. Il fatto che un indirizzo appartenga alla black list non implica necessariamente che i messaggi da esso provenienti debbano essere sempre bloccati. Piuttosto, **viene aumentato il punteggio di spam** di tali messaggi e molti di essi vengono bloccati solo dai controlli successivi. Solo i messaggi con un punteggio molto basso non vengono classificati come spam.

Il concetto opposto si applica alle white list del filtro AntiSpam. Le **white list** identificano infatti gli **indirizzi email che hanno scarsa possibilità di essere sorgenti o destinatari di spam**.

Tuttavia, essere in una white list non esime un indirizzo dal processo AntiSpam. Piuttosto, viene regolato il punteggio assegnato ai messaggi ad esso diretti o ad esso inviati, affinché la maggior parte di questi **non venga bloccata**. Solo i messaggi con un punteggio molto alto vengono classificati come spam.

Le **liste di esclusione**, per il filtro AntiSpam, contengono quegli **indirizzi email che vengono esentati dal processo**. Per esempio, le email provenienti dagli indirizzi registrati nelle rubriche personali degli utenti possono essere esonerate dal processo AntiSpam.

HashCash e i francobolli elettronici

A causa della piccola percentuale di risposte ottenute, gli spammer hanno bisogno di inviare email in grande quantità. Più velocemente inviano i loro messaggi, maggiori sono le occasioni di vendita.

Una tecnologia emergente denominata **Hash-**

Cash inserisce una sorta di “francobollo” elettronico nei messaggi email legittimi. La presenza di questo francobollo (*stamp*) in una email indica che si è impiegato tempo per creare e inserire un “francobollo” in un determinato messaggio che quindi, presumibilmente, non sarà spam.

HashCash rallenta, seppur leggermente, i tempi di invio delle email, cosa che gli spammer non possono permettersi.

La tecnologia HashCash permette di legittimare le email che non sono spam. Maggiore è il “valore” del francobollo, maggiore è il tempo di elaborazione che è stato impiegato per inviare il messaggio che quindi, verosimilmente, non sarà spam.

MDaemon è in grado sia di creare i francobolli elettronici per inviare i messaggi, sia di leggere i francobolli dei messaggi in ingresso.

Outbreak Protection

SecurityPlus for MDAemon è il plug-in di MDAemon che arricchisce le funzionalità antispam del mail server, grazie alla rivoluzionaria tecnologia Outbreak Protection.

Outbreak Protection consente di intercettare e fermare il malware prima ancora che siano rese disponibili le relative segnature. In questo modo Outbreak Protection rafforza la sicurezza di MDAemon anche nei confronti dei cosiddetti attacchi “del giorno zero”, i più insidiosi.

Principali caratteristiche degli strumenti AntiSpam di MDAemon

DNS Black List

- Attivazione del controllo DNS Black List.
- Classificazione dei messaggi provenienti dai siti elencati nelle black list.
- Controllo delle intestazioni “Received” per i messaggi SMTP o POP.
- Controllo opzionale le intestazioni “received” per gli indirizzi inseriti nelle white list.
- Aggiunta, modifica e cancellazione dei server che ospitano le DNS Black List.
- Mantenimento in cache dei risultati dei controlli delle DNS Black List.
- Esenzione dai controlli per i siti appartenenti alle white list.

Controlli SPF/Sender-ID

- Attivazione dei controlli SPF/Sender-ID.
- Elaborazione delle intestazioni “From” dei messaggi.
- Aggiunta dell’intestazione “Received-spf” nei messaggi.
- Impostazione delle opzioni per i test SPF con risposta “fail”.
- Impostazione dei punteggi di spam per i diversi risultati ottenuti con il controllo SPF.

- Esenzione delle sessioni autenticate dal controllo SPF/Sender-ID.
- Esenzione degli IP sicuri (trusted) dal controllo SPF/Sender-ID.
- Mantenimento nella cache dei risultati del controllo SPF/Sender-ID.

Greylisting

- Attivazione e disattivazione del controllo Greylisting.
- Modifica dei tempi di entrata in funzione di Greylisting.
- Modifica del tempo di permanenza nel database degli indirizzi email.
- Esenzione dei controlli per particolari indirizzi o domini.
- Opzioni per mitigare gli effetti collaterali.
- Integrazione con SPF/Sender-ID.

Filtraggio spam

- Impostazione delle opzioni per l’elaborazione dei messaggi etichettati come spam.
- Esenzione degli indirizzi locali, sicuri (trusted) e autenticati.
- Esenzione dal controllo dei messaggi più grandi di una dimensione specificata (fino a 2 MB).

- Blocco dell'inoltro per i messaggi etichettati come spam.
- Smistamento automatico dello spam in opportune cartelle IMAP degli utenti.
- Attribuzione del punteggio di spam per le black list e le white list.

DomainKeys Identified Mail

- Attivazione e disattivazione del DKIM sui messaggi in ingresso.
- Attivazione e disattivazione del DKIM sui messaggi in uscita.
- Attivazione dei controlli per particolari indirizzi o domini.
- Generazione di chiavi pubbliche e private internamente a MDAemon.
- Attribuzione di punteggi spam ai messaggi in base al risultato del controllo DKIM.

Analisi euristica

- Attribuzione dei punteggi di spam per il processo euristico.
- Impostazione della soglia per il punteggio di spam.
- Impostazione della soglia del punteggio di spam per rifiutare i messaggi SMTP e mostrare i risultati dell'analisi euristica in appositi log SMTP.
- Modifica del messaggio di avviso contenuto nell'oggetto dei messaggi classificati come spam.

Classificazione bayesiana

- Applicazione della tecnologia bayesiana al sistema di punteggio euristico.
- Attivazione dell'"apprendimento" bayesiano periodico.
- Attivazione manuale dell'"apprendimento" bayesiano.

- Impostazione delle cartelle pubbliche dove salvare esempi di email legittime e di spam.

Opzioni di reportistica

- Impostazione delle opzioni di reportistica per i messaggi etichettati come spam.
- Inserimento dei report nelle intestazioni dei messaggi originali.
- Creazione di un nuovo messaggio a cui allegare l'originale.
- Creazione di un nuovo messaggio a cui allegare l'originale in formato di solo testo.

HashCash e francobolli elettronici

- Inserimento di "francobolli" nei messaggi in uscita (HashCash).
- Uso di francobolli (HashCash) solo nelle sessioni SMTP autenticate.
- Aggiunta, modifica e cancellazione di indirizzi nella Mint List (lista degli indirizzi alle cui email va applicato il "francobollo").
- Impostazione del valore dei francobolli elettronici, modificando il "peso" dello stamp.
- Controllo dei francobolli elettronici (HashCash) dei messaggi in ingresso.

Black List, White List e liste di esclusione

- Aggiunta, modifica e cancellazione degli indirizzi nelle black list, white list (To) e white list (From).
- Attivazione della white list generata dalla rubrica.
- Attivazione dell'aggiornamento automatico degli indirizzi.
- Aggiunta dei messaggi non-spam alla cartella che contiene gli esempi di email legittime per l'apprendimento bayesiano.
- Attivazione dell'indirizzo email per l'inoltro di messaggi delle white list.

Achab S.r.l. - Piazza Cinque Giornate, 4 - 20129 Milano
Tel: 02 54108204 - Fax: 02 5461894 - <http://www.achab.it>
Informazioni commerciali: sales@achab.it
Informazioni tecniche: supporto@achab.it