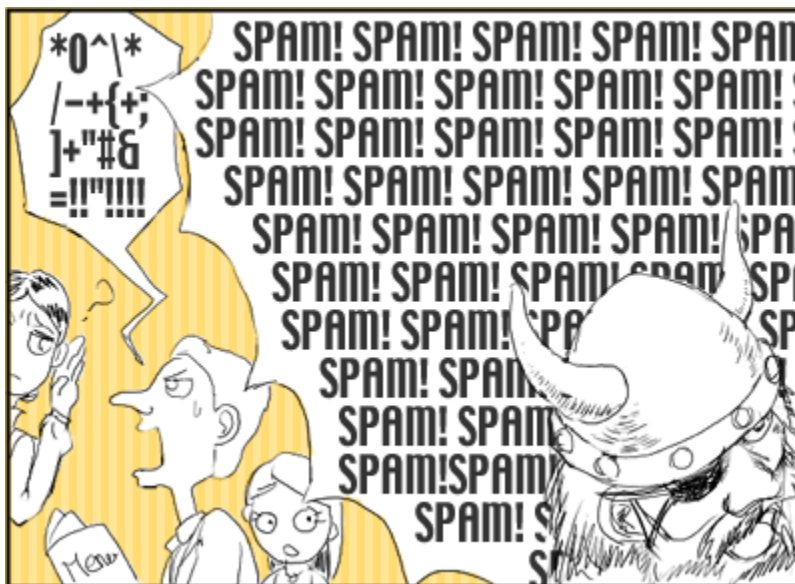


Spam & Tecniche Antispam

- Andrea Cavenago -



Da Wikipedia:

"...Il termine trae origine da uno sketch comico del Monty Python's Flying Circus ambientato in un locale nel quale ogni pietanza proposta dalla cameriera era a base di Spam (un tipo di carne in scatola). Man mano che lo sketch avanza, l'insistenza della cameriera nel proporre piatti con "spam" ("uova e spam, uova pancetta e spam, salsicce e spam" e così via) si contrappone alla riluttanza del cliente per questo alimento, il tutto in un crescendo di un coro inneggiante allo "spam" da parte di alcuni Vichinghi seduti nel locale. La reiterazione ossessiva della parola nella canzone ha poi portato all'uso dello stesso termine per indicare le e-mail commerciali non richieste."



SOMMARIO

1	Introduzione.....	3
2	Rubare gli indirizzi email.....	4
2.1	SpamBot.....	4
2.2	Trojan.....	5
2.3	Indirizzi Inventati.....	5
3	Ottenere conferma degli indirizzi email.....	7
4	Invio (massiccio) di posta elettronica	8
4.1	Email Server.....	8
4.1.1	Email Header.....	10
4.2	Open-Relay Mail Server & Open Proxy.....	12
4.3	Zombie Spam.....	13
5	Tecniche per bloccare lo Spam	14
5.1	BlackList & WhiteList.....	14
5.2	Filtri Statici	18
5.3	Filtri Statistici	18
5.4	Blocco dello spam a livello del singolo client	21
5.4.1	Mozilla ThunderBird.....	21
5.4.2	Microsoft Outlook Express.....	21
5.4.3	Microsoft Outlook 2003.....	21
6	Altri metodi di Spam.....	23
6.1	Forum.....	23
6.2	Newsgroup.....	24
7	Statistiche.....	26
8	Conclusioni.....	26

1 Introduzione

Con il termine spam si indicano generalmente quelle email, principalmente di pubblicità, che ci sono inviate da utenti/società anonime e per le quali non abbiamo fatto una esplicita richiesta.

Una definizione più dettagliata, conosciuta da una delle società che quotidianamente combatte lo spam, è la seguente:

“Un messaggio elettronico è definito “spam” **SE**: (1) l’identità personale del destinatario ed il contesto sono irrilevanti poiché il messaggio è ugualmente applicabile ad altri potenziali destinatari; **E** (2) il destinatario non ha nessuna prova di aver dato un permesso deliberato, esplicito e sempre revocabile di voler ricevere tale messaggio; **E** (3) la trasmissione e ricezione del messaggio agli occhi del destinatario danno vantaggi sproporzionati al mittente.”ⁱ

Analizzando bene tale definizione si rileva che in effetti un messaggio di spam cerca di raggiungere il più alto numero di destinatari possibili, senza tener conto della tipologia di persona che sta ricevendo tale messaggio (e quindi diversamente dalla normale pubblicità dei media tradizionali, che si rivolge a ben determinate fasce di pubblico), in via del tutto arbitraria e senza possibilità di scelta se ricevere o meno tali messaggi, ed ovviamente dando benefici al mittente il quale, contando su fatti probabilistici, cerca di raggiungere il più alto numero di destinatari in modo da avere probabilità più alte sul fatto che comunque qualcuno acquisterà o visiterà il sito del prodotto/servizio proposto.

Chiunque abbia una casella email avrà sicuramente ricevuto almeno una volta un messaggio di spam, ove per l’appunto veniva reclamizzato un medicinale o un qualche altro prodotto o servizio. Il primo pensiero che ci viene in mente alla vista di tali messaggi è cercare di capire come ed in che modo hanno avuto il nostro indirizzo di posta, cercando a ritroso se per caso abbiamo inserito il nostro indirizzo email in qualche form durante la nostra navigazione in qualche sito.

Scopo del presente documento è quello di offrire una panoramica di tutto ciò che è legato al fenomeno dello spam, e cioè partendo dal modo con cui vengono raccolti gli indirizzi email fino al modo con cui vengono inviati i messaggi agli indirizzi raccolti, illustrando anche i principali metodi utilizzati per arginare e combattere tale fenomeno.

2 Rubare gli indirizzi email

Ogniqualvolta ci registriamo presso un sito web forniamo, oltre ai dati personali, anche il nostro indirizzo email.

E' una procedura corretta poiché è il metodo più comodo per metterci in contatto col manutentore del sito stesso, ad esempio sia per richiedere che per ottenere assistenza (classico esempio: "*Password dimenticata?*").

Se il sito presso cui ci iscriviamo è considerato sicuro, possiamo essere tranquilli che la nostra email sarà in "buone mani", e cioè che, come spesso il sito stesso dichiara, verrà utilizzata solamente per comunicazioni ufficiali e non verrà ceduta a terze parti senza il nostro esplicito consenso.

A volte la superficialità con cui utilizziamo l'indirizzo email ci fa cadere invece nell'errore di **inserirlo anche in siti web** che non sono proprio un esempio di correttezza ed onestà, andando a popolare il database di società e/o privati che utilizzeranno tali indirizzi email per scopi non propriamente onesti.

Ovviamente con un pò di buon senso è facile evitare di regalare così il nostro indirizzo email; come conseguenza gli spammer si sono fatti più furbi, ed hanno cominciato a sfruttare le risorse che internet mette a disposizione per raccogliere indirizzi di posta elettronica in maniera veloce e trasparente.

2.1 SpamBot

Un newsgroup, una chat oppure un forum contengono spesso l'indirizzo email dell'utente che sta scrivendo o che ha postato il messaggio, quindi per uno spammer è sufficiente utilizzare tali servizi per aggiudicarsi un bel bottino di indirizzi email.

Ma perché perdere tempo prezioso navigando a destra e manca quando un semplice programmino può farlo al posto nostro? Appositi programmi chiamati "**spambot**" girano per la rete alla ricerca di indirizzi di posta elettronica sfruttando il fatto che un indirizzo email ha un semplice formato riconoscibile.

Tali spambot cominciano la ricerca da una pagina web, e la analizzano alla ricerca della stringa "*mailto:*" che identifica, nella codifica HTML, un indirizzo di posta elettronica all'interno della pagina stessa. Trovato l'indirizzo email, esso viene salvato per futuri utilizzi mentre il bot segue gli hyperlink presenti all'interno della pagina stessa per raggiungere nuove pagine da analizzare, e così via. Tale processo viene ripetuto potenzialmente all'infinito. Il funzionamento degli spambot è simile a quello degli spider (o webcrawler) usati dai principali motori di ricerca; essi sono dei programmi che attraversano il web alla continua ricerca di pagine da inserire nei propri archivi.

Gli spambot possono essere utilizzati sia all'interno delle pagine web, sia all'interno dei newsgroup, sia all'interno di eventuali chat: il funzionamento è praticamente lo stesso.

Il principale metodo utilizzato dagli utenti contro gli spambot consiste nel "camuffare" (spesso viene usato il termine "*address munging*") l'indirizzo email in modo da ingannare il bot. Il camuffamento può consistere nell'aggiungere dei caratteri o delle stringhe nell'indirizzo, oppure sostituire il simbolo @ con il suo significato, e cioè con at, <at>, ecc. Un bot avrà difficoltà a riconoscere un indirizzo valido, mentre un normale utente lo interpreterà correttamente. Altro metodo consiste nell'inserire il proprio indirizzo email sotto forma di immagine; nessuno spambot è (per ora) in grado di interpretare il contenuto di una immagine ed estrarre da esso l'indirizzo email.

Esempio 1: andrea@<remove-this>miodominio.it

Esempio 2: andrea<AT>miodominio.it

Esempio 3: andrea@miodominio.it

Nell'esempio 1, il bot rileverà un indirizzo email per lui valido, ma quando gli invierà un messaggio, si verificherà un errore; un utente "umano" invece rimuoverà la stringa <remove-this> per ottenere l'indirizzo corretto; ognuno è libero di interporre la stringa che vuole, l'importante è che sia chiaro quale è la parte estranea dell'indirizzo che quindi andrà eliminata. Nell'esempio 2 invece lo spambot non rileverà nessun indirizzo poiché quanto riportato non rispecchia i normali canoni per gli indirizzi di posta elettronica, e cioè in questo caso manca il simbolo "@". Nell'esempio 3 è invece riportata una immagine .jpg contenente l'indirizzo email; come riportato sopra, al momento nessun bot è in grado di analizzare le immagini e di estrapolare da esse gli indirizzi email (o per lo meno non conviene loro analizzare ogni immagine per verificare se è un indirizzo email).

2.2 Trojan

Spesso siamo sicuri di non aver mai usato il nostro nuovo indirizzo email su internet, ma di averlo dato solamente a qualche amico, e ci troviamo comunque invasi di messaggi di spam. Tra le possibili cause è da tenere in considerazione il fatto che magari qualcuno degli amici cui abbiamo dato il nostro nuovo indirizzo ha inavvertitamente installato un trojan, che a sua insaputa gli ha "rubato" i contatti di posta elettronica presenti sul suo computer.

Un trojan non è altro che un programma all'apparenza innocuo (ad es. un piccolo videogioco, o un programmino che visualizza qualcosa di carino, come gli auguri di Natale ecc.) che in realtà nasconde al suo interno un programma ben più pericoloso. Tale programma può fare potenzialmente qualsiasi cosa, e nel nostro caso lo spammer che l'ha inviato lo utilizza per carpire gli indirizzi di posta elettronica del nostro amico.

2.3 Indirizzi Inventati

Altro metodo utilizzato consiste nell'inventare l'indirizzo email, utilizzando pattern comuni che spesso la gente utilizza come email address, e modificando successivamente il dominio di destinazione. Tali pattern possono essere i nickname più utilizzati, così come la combinazione di nome e cognome (molti provider utilizzano un metodo del genere per creare l'indirizzo email da suggerire all'utente stesso durante la fase di registrazione).

Ad esempio uno spammer potrebbe provare a spedire spam a Mario Rossi, ipotizzando un email address del tipo *mrossi*, e associandolo poi a diversi domini (*mrossi@tin.it*, *mrossi@libero.it*, *mrossi@hotmail.com*, ecc).

3 Ottenere conferma degli indirizzi email

Lo spammer quando invia una email ovviamente non richiede la notifica di lettura da parte del ricevente, né tanto meno inserisce informazioni, nel messaggio, che permettano di risalire a lui. Per validare quindi l'indirizzo del destinatario occorre puntare su altre risorse, le quali sono:

1. Link ad immagini esterne presenti nella email,
2. Ingenuità dell'utente.

Il primo metodo si verifica solamente con i messaggi email scritti in HTML e consiste nell'inserire nella email uno o più link a immagini vere e proprie, oppure a piccole immagini trasparenti di appena 1 pixel per 1 pixel di dimensione. La riga di codice HTML che dovrebbe richiamare direttamente l'immagine richiama in realtà uno script (presente su un server cui lo spammer ha accesso) e al quale è associato in ingresso un identificativo (o nel peggiore dei casi sarà presente direttamente l'indirizzo email); tale identificativo è associato, in un database sul server, al nostro indirizzo di posta elettronica. Lo spammer così può convalidare il nostro indirizzo di posta come attivo e regolarmente consultato.

Esempio 4:

```
<IMG height=1 src="http://spammer.com/cgi-bin/email.pl?id=12345" width=1>
```

Nell'esempio sopra, il link che dovrebbe richiamare direttamente l'immagine in realtà richiama uno script in Perl chiamato email.pl e che risiede sul server "spammer.com". A tale script è passato come parametro di input l'identificativo "12345" che corrisponderà, in un apposito database presente sul server, al nostro indirizzo di posta elettronica. A volte succede che al posto dell'identificativo appaia come parametro in input dello script il nostro indirizzo email. In questo modo non facciamo altro che confermare la bontà del nostro indirizzo email oltre al fatto che è regolarmente consultato.

Attualmente la maggioranza dei client di posta permette di impostare livelli di protezione che permettono di effettuare il download a immagini su siti esterni solamente se il mittente è fidato (cioè inserito nella whitelist dell'utente) oppure solamente previa conferma del destinatario, che decide di volta in volta se visualizzare le immagini collegate oppure no. Una protezione simile è svolta anche per i link a indirizzi esterni, che molti client di posta disabilitano onde evitare che vengano cliccati inavvertitamente.

Il secondo metodo, molto più semplice e subdolo, sfrutta l'ingenuità del ricevente, e cioè nella email vi è un messaggio che lo informa che se non vuole più ricevere tali comunicazioni gli è sufficiente rispondere alla presente email per essere tolto dall'elenco dei destinatari; ovviamente tale gesto (cioè la risposta) non fa altro che confermare allo spammer della validità dell'indirizzo email (oltre al fatto di dimostrare che tale indirizzo è regolarmente consultato), e che quindi tale indirizzo è da considerare come futuro bersaglio di spam. Per evitare di cadere in questa trappola occorre prestare sempre molta attenzione a tali email, cercando di controllare quanti più dati possibili tra i quali il mittente, lo header, il messaggio riportato ecc.

4 Invio (massiccio) di posta elettronica

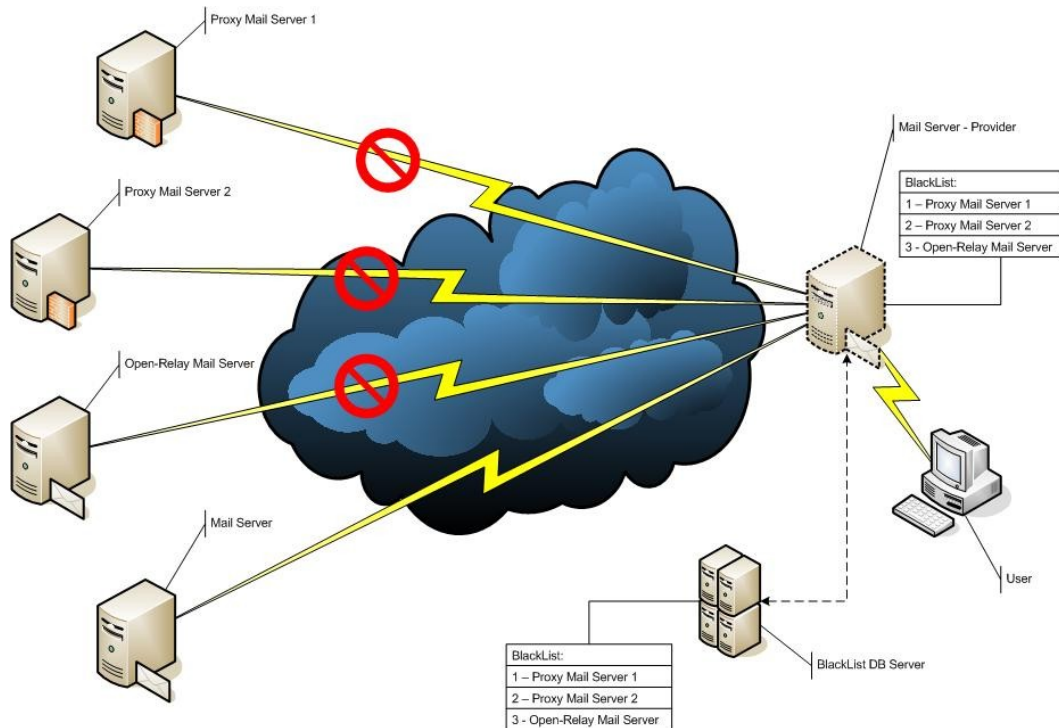
Ottenuti gli indirizzi email, il passo successivo consiste nell'inviare centinaia di migliaia di messaggi di posta elettronica nel più breve tempo possibile, cercando di nascondere le proprie tracce per evitare di poter essere individuati. In questo capitolo sarà illustrato brevemente il funzionamento del servizio di posta elettronica e verrà descritto l'Header di un messaggio di posta, tramite il quale sarà poi possibile creare degli appositi filtri antispam.

4.1 Email Server

I server di posta elettronica (o *MTA, Mail Transfer Agent*) vengono utilizzati quotidianamente da milioni di utenti per inviare e ricevere email. Essi si appoggiano su due protocolli fondamentali quali il POP (Post Office Protocol) per il prelievo di posta ed il protocollo SMTP (Simple Mail Transfer Protocol) per l'invio. Benché i protocolli siano diversi, capita spesso che il server POP ed il server SMTP risiedano sulla stessa macchina (operano su porte differenti) e diversamente dal protocollo SMTP, il protocollo POP richiede una autenticazione mediante user e password per poter scaricare la posta elettronica.

Quando un utente vuole inviare della posta elettronica compone il messaggio col proprio client (o *MUA, Mail User Agent*) e lo invia ad un server di posta elettronica SMTP; il server SMTP si prende carico di "scoprire" dove si trova il destinatario e di inviare il messaggio email al suo server di posta. Per poter inviare una email dobbiamo eseguire uno scambio di informazioni con il server di posta, e per semplificarci la vita il client svolge per conto nostro questo scambio, e fornisce al server informazioni quali il mittente (cioè noi) il/i destinatario/i, il messaggio stesso ed altri dati. Ricevuto il messaggio, il mail server lo instrada o direttamente al mail server del destinatario, o verso altri server che si preoccuperanno di inoltrarlo alla destinazione, e cioè al mail server del destinatario. Con comodo, il destinatario userà il proprio MUA per accedere al proprio MTA per poter scaricare il messaggio sul proprio computer. Per nostra fortuna ogni server attraversato aggiunge importanti informazioni al messaggio, andando a modificare l'Header (intestazione) del messaggio stesso di posta elettronica.

Esempio 5: Comunicazione MUA - MTA



4.1.1 Email Header

Durante il suo tragitto, l'email può attraversare altri server di posta che si preoccupano di smistare il messaggio, aggiungendo delle informazioni nello Header (intestazione) della email. Infatti un messaggio di posta elettronica contiene, oltre al messaggio, al mittente e ai destinatari, anche altre informazioni che permettono di verificare il percorso effettuato dal messaggio a partire dal mittente per giungere al destinatario. Ciascun server che il messaggio attraversa aggiunge delle informazioni nella intestazione del messaggio stesso, specificando da chi ha ricevuto il messaggio (indirizzo IP e nome host) e data e ora in cui il messaggio è arrivato al server in questione, più qualche altra informazione sul software installato sul server. Queste informazioni vengono inserite nello Header del messaggio.

Un esempio di Header è il seguente:

```
Received: from aa024msr.fastwebnet.it (10.31.174.100) by cpmsres03.intranet.fw
(7.3.104) id 44F751CB00B71E1C for xxx.yyy@fastwebnet.it; Sat, 16 Dec 2006
14:59:26 +0100

Received: from dti.unimi.it (159.149.70.113) by aa024msr.fastwebnet.it
(7.3.105.6) id 4541C54A083BD442 for xxx.yyy@fastwebnet.it; Sat, 16 Dec 2006
14:59:25 +0100

Received: from [159.149.71.122] ([159.149.71.122] verified) by dti.unimi.it
(CommuniGate Pro SMTP 4.2.10) with ESMTP id 6436729 for xxx.yyy@fastwebnet.it;
Sat, 16 Dec 2006 14:58:43 +0100
```

- Il primo *Received* ad essere stato aggiunto è quello scritto in blu, in basso; esso ci dice che il messaggio email è stato ricevuto dal server dti.unimi.it, sul quale è in esecuzione il software di posta "CommuniGate Pro SMTP 4.2.10", da un host avente indirizzo IP 159.149.71.122, oltre all'indirizzo email del destinatario, l'orario di ricevimento e la data.
- Il secondo *Received* (in rosso, a metà) è stato aggiunto dal server di posta elettronica del mio attuale provider (fastweb) chiamato aa024msr.fastwebnet.it, il quale ha ricevuto il messaggio dal server dti.unimi.it avente indirizzo IP 159.149.70.113, oltre nuovamente all'indirizzo email del destinatario, l'orario di ricevimento e la data.
- Il terzo *Received* (in verde, in alto) è stato aggiunto da un ulteriore server di posta elettronica, l'ultimo, al quale il mio computer si è collegato per scaricare la posta; corrisponderà al server pop che ho impostato nella proprietà del mio account di posta elettronica.

Queste sono le informazioni che lo spammer non può falsificare, a meno che non possa intervenire sui server (o alcuni di essi) che il messaggio attraversa. Gli altri campi, quali l'indirizzo email del mittente e del destinatario, e cioè quelli che un utente vede apparire nella email ricevuta, possono tranquillamente essere manomessi e falsificati dallo spammer, che non avrebbe nessun interesse a mettere il proprio indirizzo email come mittente.

Queste informazioni ci sono di aiuto, poiché ci permettono di poter avvisare un eventuale provider che un suo abbonato sta inviando spam, oltre al fatto che è possibile cancellare o etichettare il messaggio come spam se ha attraversato un mail server contenuto in una qualche blacklist.

4.2 Open-Relay Mail Server & Open Proxy

Per motivi di sicurezza nella maggior parte dei casi l'invio di posta elettronica deve avvenire esclusivamente mediante i server SMTP messi a disposizione dall'ISP con cui si è attualmente collegati ad internet. Tale controllo è svolto dagli ISP in modo da permettere solamente ai propri clienti/abbonati l'utilizzo dei propri server SMTP; questa soluzione è già un primo passo per combattere lo spam in quanto per registrarsi presso un Internet Service Provider occorre fornire informazioni e dati personali ed è quindi più difficile risultare completamente anonimi. Tale controllo è solitamente fatto in base all'indirizzo IP assegnato al client (e cioè "se il tuo IP address appartiene a quelli assegnati ai miei abbonati, allora sei un mio abbonato e puoi usare il mio server SMTP per inviare i tuoi messaggi email"). Altro metodo di controllo permette all'utente di inviare posta (quindi di usare il protocollo SMTP) solamente se prima si è autenticato con il protocollo POP; in pratica il server di posta memorizza l'indirizzo IP del client nel momento in cui si autentica per il prelievo, e successivamente permette al client con tale indirizzo IP di poter utilizzare il protocollo SMTP per inviare posta. Tale metodo, conosciuto con **POP-before-SMTP**, richiede che l'utente abbia una login ed una password per poter ricevere/inviare posta, negandone l'invio quindi a chi non ha un regolare account presso il provider.

Lo stesso discorso si può fare per le aziende, le quali configurano (o *dovrebbero* configurare) i loro server di posta per permettere l'invio di posta, tramite i propri mail server, ai soli dipendenti.

Succede però che certe volte i controlli sopra descritti non sono messi in atto, vuoi per colpa di una svista, per un errore di configurazione, per semplice ingenuità oppure anche volutamente; come conseguenza si ottengono degli **open-relay mail server**, cioè dei server di posta che non applicano nessun controllo sui mittenti delle email che lo attraversano, permettendo a chiunque di inviare posta elettronica tramite essi. Non è necessaria quindi nessuna autenticazione e/o appartenenza ad una determinata subnet di indirizzi IP per poterli utilizzare, e per questo motivo sono utilizzati dagli spammer per l'invio di enormi quantità di posta. L'utilizzo, da parte dello spammer, di un open-relay mail server non gli garantisce l'anonimato in quanto il suo indirizzo IP sarà comunque inserito nello Header della email dal server di posta open-relay. Lo spammer quindi dovrà escogitare dei metodi per evitare di essere rintracciato.

Gli **open proxy** sono invece utilizzati per mantenere l'anonimato in rete. Abbiamo descritto precedentemente che mediante le informazioni contenute nello Header di un messaggio di posta è possibile ottenere gli indirizzi IP dei server che il messaggio ha attraversato, permettendo quindi di risalire all'indirizzo IP dello spammer, o comunque ad un IP molto vicino ad esso.

Utilizzando un open proxy le informazioni inserite nello Header inizieranno con quelle inserite dall'open proxy, mentre quelle precedenti (cioè dal client dello spammer) non saranno inserite; in pratica guardando lo header è come se l'email ci fosse stata spedita direttamente dal proxy. Il termine "open" indica che per poter utilizzare questo servizio non è richiesta nessuna particolare autenticazione e/o requisito.

Lo spammer quindi utilizza open-relay mail server o open proxy in modo da evitare di essere scoperto, o per lo meno per rendere arduo questo compito.

Occorre dire innanzitutto che gli open-relay mail server possono essere evitati configurando adeguatamente il proprio server; addirittura molti siti offrono servizi di verifica che permettono di controllare se un server di posta (ad esempio il nostro) è un open-relay oppure no. Se però tale tipo di server lo si è voluto creare volutamente, allora l'unico mezzo di difesa è quello di inserirlo in apposite blacklist, in modo da bloccare tutte le email che arriveranno da esso, le quali saranno con altissima probabilità solamente spam. Lo stesso discorso lo si può fare per gli open proxy, per i quali l'unico metodo di filtraggio è appunto la blacklist.

4.3 Zombie Spam

Anche i singoli PC degli utenti si possono trasformare in mittenti di messaggi di spam, e quando ciò avviene si hanno degli "**zombie spam**", cioè dei normali client che a causa di malware installato tramite qualche trojanhorse cominciano ad inviare email di spam a chiunque.

Tale problema risulta difficile da gestire in quanto gli ISP non possono basarsi sulle normali blacklist (liste contenenti noti domini che generano spam, e che quindi sono filtrati e bloccati – Rif. § 5.1 – "BlackList & WhiteList") poiché ciò risulterebbe in un blocco totale di scambio di email tra utenti con ISP differenti.

L'unica soluzione (neanche molto elegante) a tale problema sarebbe quella di far sì che l'ISP permetta a ciascun client di inviare un numero limitato di email al giorno, oppure di bloccare l'invio di email sino a che l'utente stesso non avrà ripulito il proprio computer togliendolo dallo stato di "zombie".

Il possessore del computer si potrà rendere conto di ciò solamente analizzando il traffico generato in uscita, ma se non ha particolare "confidenza" con gli strumenti informatici, ecco che un computer zombie può rimanere tale per un lungo periodo di tempo.

L'unico modo per evitare di divenire uno Zombie Spam è prima di tutto quello di non installare applicazioni scaricate da internet e delle quali non sappiamo nulla, così come evitare di aprire allegati a mail sconosciute. Così facendo eliminiamo alla radice il problema di avere un trojan sul nostro computer che possa installare qualunque genere di programma. Anche l'installazione di patch critiche di software e/o sistema operativo può contribuire a rendere più resistente il nostro computer da attacchi che sfruttano le vulnerabilità.

Nel caso sia troppo tardi, ci si può accorgere di essere divenuto uno zombie spam analizzando il traffico di rete (che sarà cospicuo) o rilevando comportamenti anomali della macchina (lentezza soprattutto), oppure venendo informati dal proprio ISP che avrà rilevato un abnorme invio di email da parte del nostro computer.

5 Tecniche per bloccare lo Spam

Escludendo il comune buon senso che ci evita di inserire l'indirizzo email in ogni form che incontriamo, altre tecniche più o meno sofisticate sono nate per arginare il fenomeno dello spam; di seguito ne verranno illustrate le principali, che comprendono sia quelle adottate dagli ISP che quelle adottate nei principali client di posta elettronica.

5.1 BlackList & WhiteList

Le blacklist e le whitelist sono il primo muro di difesa contro lo spam, e consentono di "scremarne" una buona fetta basandosi su poche ma preziose informazioni.

Esse contengono un elenco dei domini e degli utenti che inviano spam (le blacklist) ed un elenco dei domini e degli utenti affidabili (le whitelist) e possono essere utilizzate sia a livello di ISP che a livello di singolo client (Rif. § 5.4 – "Blocco dello spam a livello del singolo client").

Solitamente le blacklist si usano quando si intende applicare una politica del tipo "*permetti il passaggio di tutto, tranne che di quanto specificato nella blacklist (default allow)*" mentre una whitelist definisce una politica del tipo "*non far passare niente che non sia presente nella whitelist (default deny)*". Ovviamente nel caso di sistemi antispam tali politiche non sono così restrittive, e cioè nel caso della whitelist se vi è un riscontro non sono applicati altri filtri (o sono applicati filtri più leggeri) mentre nel caso della blacklist se vi è riscontro il messaggio viene bloccato altrimenti il messaggio viene comunque analizzato da altri filtri.

ORDB:

Oltre a poterle creare e gestire localmente, vi sono numerose società (a pagamento e gratuite) che raccolgono e gestiscono dei veri e propri database contenenti domini che effettuano spamming; tali database sono comunemente chiamati ORDB (Open Relay Data Base). Un ISP o una azienda possono sfruttare questo servizio per effettuare un controllo sulla posta in arrivo senza quindi preoccuparsi di dover gestire le blacklist al loro interno. Ovviamente un servizio del genere comporta un certo rallentamento, benché le query siano inviate parallelamente a più server; infatti, c'è da considerare che deve essere fatta una richiesta, la quale deve giungere al server contenente il DB, sul quale viene fatta una query, il cui risultato deve poi essere spedito al richiedente, e solo allora il messaggio potrà giungere a destinazione o al filtro seguente.

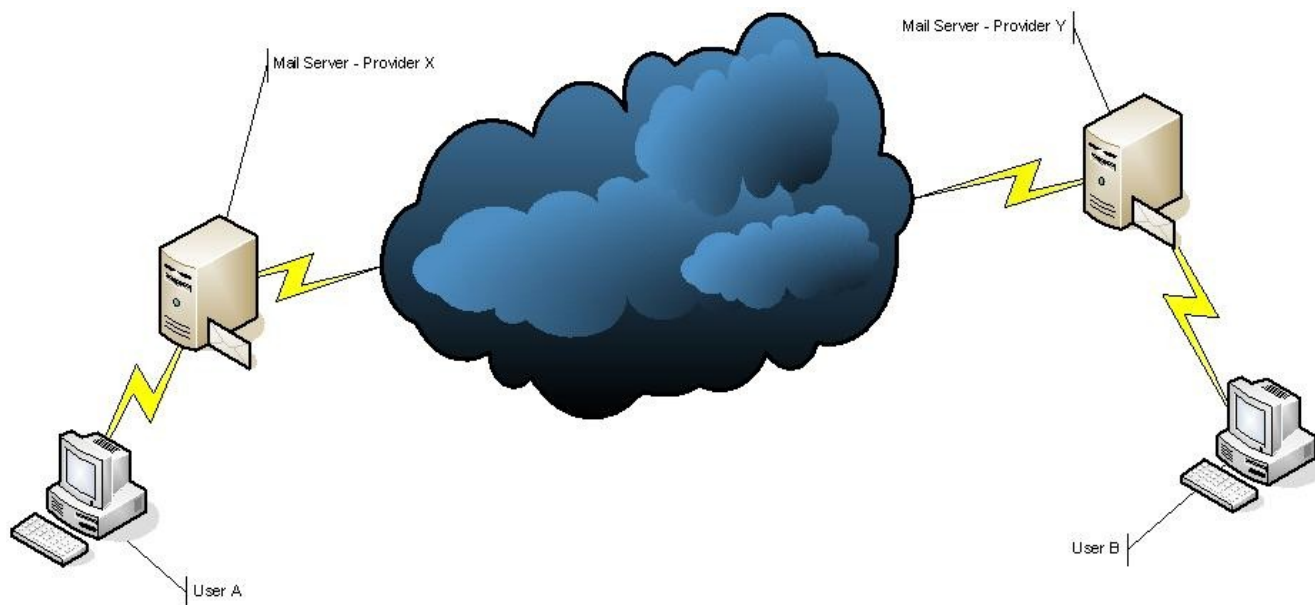
Hashing:

Oltre al sistema di blocco basato sui domini, esiste un altro metodo che sfrutta il sistema delle blacklist ma che però opera sull'hash (indicato anche come 'checksum' in alcuni riferimenti) di ciascuna singola email di spam; l'hash è generato da una apposita funzione e permette di ottenere una sorta di impronta digitale del messaggio, univoca per ciascun messaggio dato in input a tale funzione. Supponiamo ora che il nostro sistema antispam riceva una email; se configurato opportunamente, effettuerà una query per l'hash di quella email presso un server che effettua tale servizio. Se in tale server era già stata inserita l'hash per quella mail di spam, avremo un riscontro ed il nostro messaggio verrà etichettato come spam, andando ad alimentare il nostro filtro statistico. Lo svantaggio di un sistema del genere risiede nel fatto che molto spesso le email di spam sono inviate in modo massiccio in brevi intervalli di tempo, quindi è possibile che nel momento in cui il nostro sistema antispam esegue la query al server, l'hash di tale email non sia ancora stata inserita nel database.

Tornando alle liste, il tipo più comunemente usato è la blacklist in quanto è più semplice da gestire, a livello globale, rispetto ad una whitelist. Infatti, gli appartenenti ad una blacklist sono

una minima percentuale rispetto ai domini leciti presenti al mondo, mentre se si usasse una whitelist occorrerebbe inserire tutti i domini leciti, cosa impossibile da gestire. Il discorso può comunque non essere vero se riportato al singolo client o alla singola lan, nelle quali magari per esigenze particolari si specifica di voler ricevere email solamente da determinati indirizzi o domini, filtrando tutte le altre email che non corrispondono ai criteri.

Esempio 6: Funzionamento di una BlackList per un mail server



Con l'uso di tali liste si possono mettere in pratica dei filtri netti ma anche potenzialmente pericolosi. Qualche anno fa una famosa compagnia americana di servizi business-to-business, la **iBill**, venne inserita in una blacklist da una altrettanto nota società, **MAPS (Mail Abuse Prevention System)**, che si occupa di gestire le blacklist per la metà degli ISP americani. Qualcuno si è lamentato presso la MAPS che un cliente della iBill inviava spam; la MAPS, dopo un controllo, ha messo nella propria blacklist sia il cliente della iBill che un intero blocco di 254 indirizzi IP della iBill stessa, con conseguente blocco di alcuni servizi per quattro giorni e perdite stimate in 400.000 \$ⁱⁱ.

Forse questo è solamente un caso isolato, e meriterebbe di essere analizzato con cura verificando come si è giunti a tale soluzione. Ora la domanda che ci si pone è: come si può finire in una blacklist?

Innanzitutto come descritto precedentemente, le blacklist sono gestite da apposite società, quali ad esempio la sopra citata **MAPS**, oppure **Spamhaus** e **SpamCop**, le quali offrono poi i propri servizi agli ISP ed agli utenti finali (ad esempio email filtrate).

Tali società, su richiesta di utenti/società/ISP si occupano di verificare se un determinato host o server di qualche privato/società/ente sta inviando spam. Poiché tale invio può anche essere inconsapevole (come ad esempio gli zombie spam descritti precedentemente – Rif. § 4.3 – "Zombie Spam") essi cercano di contattare in qualche modo, e sulla base delle informazioni che anno, il diretto interessato. In caso di risposta assente o negativa provvedono ad inserirlo nella blacklist.

L'inserimento in una blacklist taglia fuori immediatamente il nostro indirizzo IP presso tutti gli ISP che hanno sottoscritto tale servizio, e comporta l'impossibilità di inviare email ad altre persone, poiché i server di posta che riceveranno il nostro messaggio non lo accetteranno e lo dropperanno. Come nel caso riportato sopra, molte volte non si limitano a mettere in blacklist un singolo indirizzo IP ma tutto un range, provocando problemi anche a chi con lo spam non c'entra nulla.

Le blacklist possono a loro volta essere suddivise in quattro categorie:

1. RealTime Blackhole List (RBL)
2. Dynamic User List (DUL)
3. Relay Spam Stoppers (RSS)
4. Open Proxy Stoppers (OPS)

Le RBL sono liste contenenti open relay, sorgenti di spam o servizi che supportano lo spam in generale.

Le DUL contengono utenti che utilizzano server SMTP differenti da quelli forniti loro dal proprio ISP per inviare email (come descritto precedentemente).

Gli RSS contengono indirizzi di open relay mail server, che come precedentemente illustrato permettono agli spammer di inviare posta elettronica senza nessun controllo.

Gli OPS contengono indirizzi di open proxy, i quali garantiscono un minimo di anonimato agli spammer, non aggiungendo nessuna informazione nello header.

I motivi per finire in una blacklist possono essere riassunti in:

- Invio di spam in grosse quantità (bulk email),
- Attivare sottoscrizioni a servizi senza che il cliente le abbia scelte e senza essere informato su come i suoi dati saranno usati (opt-out policy) invece che permettere al cliente di scegliere se e come sottoscrivere tali servizi (opt-in policy),
- Lasciare un open-relay mail server sul proprio network,
- Avere pagine web che sono promosse/pubblicizzate da messaggi spam,
- Fornire caselle di posta che promosse/pubblicizzate da messaggi spam (maildrop),
- Fornire banner pubblicitari, script o contatori di visite per siti promossi/pubblicizzati da messaggi spam,
- Gestire processi con carte di credito per siti promossi/pubblicizzati da messaggi spam,
- Fornire software per la distribuzione di spam,
- Ospitare pagine web di chi fornisce software per distribuire spam,
- Fornire elenchi di indirizzi email senza che il proprietario abbia dato il proprio consenso.

L'uso delle blacklist (in particolare delle RBL) sta via via diminuendo col tempo, in quanto tale metodo non permette più di combattere efficacemente lo spam come un tempo, poiché i metodi di spamming si sono nel frattempo evoluti. Un chiaro esempio è la chiusura del servizio offerto da ORDB.org, famoso Open Relay Data Base che, come asserisce nel comunicato di chiusura, afferma che "...open relay RBLs are no longer the most effective way of preventing spam from entering your network as spammers have changed tactics in recent years, as have the anti-spam community".

5.2 Filtri Statici

Uno dei primi metodi usati per bloccare lo spam, utilizzato sia dagli amministratori di sistema che dai singoli utenti sui propri client domestici, consiste nel creare dei filtri su determinate parole che notoriamente si trovano nei messaggi di spam, oppure nel creare filtri contenenti un elenco di determinati mittenti, notoriamente legati allo spam.

Quando arriva una email, se ne confronta l'oggetto, il contenuto o il mittente con quanto specificato nel filtro; se vi è riscontro positivo, l'email è considerata spam e come conseguenza viene cancellata o spostata in un apposito folder.

Tale approccio presenta due grossi problemi:

1. Aggiornamento continuo del filtro,
2. Falsi Positivi

Il primo problema lo si ha in quanto se vogliamo mantenere efficienti i filtri occorre aggiornarli spesso con nuove parole tipiche dei messaggi spam o con nuovi indirizzi di posta che inviano spam.

Il secondo problema è una conseguenza del primo, nel senso che a forza di creare filtri e popolarli con nuovi termini, si finirà per avere marchiati come spam dei messaggi che in realtà sono corretti; questo perché anche delle normali email possono avere al loro interno una o più parole che abbiamo inserito nei nostri filtri.

Prima di rimuovere messaggi contrassegnati come spam è sempre meglio verificarli, onde evitare di cancellare messaggi importanti e/o leciti.

5.3 Filtri Statistici

Per evitare i problemi esposti sopra, molti software antispam fanno uso di filtri statistici per controllare la posta in entrata. Il funzionamento di questo tipo di filtro è abbastanza semplice e permette di ottenere, a fronte di un corretto "training" iniziale del software, dei risultati abbastanza buoni.

Tali filtri statistici sono chiamati anche "Filtri Bayesiani" (da Thomas Bayes, matematico Britannico del XVIII secolo) e permettono di modificare il livello di confidenza di una data ipotesi a fronte di nuove informazioni, e cioè se a fronte delle parole contenute ho etichettato una email come spam/ham, è molto probabile che anche le successive email che conterranno tali parole dovranno essere etichettate come spam/ham.

Training Iniziale:

Sostanzialmente occorrono due liste (solitamente tabelle in un DB), chiamate ad esempio "SPAM" e "HAM". In ognuna di esse vengono inserite le parole contenute in email di spam e ham rispettivamente. Per ciascuna parola il sistema riporta anche il numero di occorrenze, quindi alla fine si otterranno due elenchi nei quali è riportato quante volte una determinata parola è apparsa in email di spam, e quante volte una determinata parola è apparsa in email di ham.

Per fare ciò l'amministratore di sistema invierà in input al sistema antispam le email considerate spam; il sistema le analizzerà ed estrarrà le parole da inserire nella lista SPAM, con relativo numero di occorrenze. Successivamente l'amministratore effettuerà lo stesso procedimento ma con le email considerate ham; anche in questo caso il sistema antispam analizzerà l'email ed

estrarrà le parole che andranno a popolare, assieme al numero di occorrenze, la lista HAM.

Per ottenere un buon training e quindi valutazioni accurate delle email, occorre processare qualche centinaio di email sia di spam che di ham. Il training è comunque un processo che non termina mai; occorre effettuare un cospicuo numero di inserimenti per poter vedere qualche risultato sul filtraggio, ma l'aggiornamento è effettuato continuamente in funzione anche del comportamento dell'utente, che può comunque etichettare come spam o ham una email che il sistema ha etichettato diversamente. In base all'etichetta assegnata dall'utente il sistema aggiorna le sue liste coi nuovi valori.

Utilizzo:

Il valore che identifica il numero di volte che una parola è contenuta in una email di spam piuttosto che di ham è utilizzato, in combinazione coi valori assegnati per gli altri token, per calcolare la probabilità che tale messaggio sia di spam o di ham.

Ogni messaggio email analizzato avrà quindi un punteggio (chiamato **score**) che è frutto di calcoli probabilistici definiti sul numero di occorrenze dei token che compongono l'email.

L'amministratore del sistema può definire la soglia entro la quale un messaggio può essere considerato spam oppure ham. Se ad esempio una email contiene una parola "ad alto rischio" spam, mentre tutte le altre sono a "basso rischio" spam, il punteggio sarà basso e quindi l'email verrà etichettata come ham.

Poiché i token comprendono anche l'header della email, la tabella HAM conterrà anche gli indirizzi email considerati affidabili, oltre ai valori di routing del messaggio (cioè da dove arriva) mentre la tabella SPAM conterrà domini e mittenti inaffidabili. In realtà questo tipo di controllo, basato su whitelist e blacklist, potrebbe essere fatto a monte mediante filtri statici sull'header; si filtrano inizialmente le email in funzione dei server che attraversano e dei mittenti. Se domini e/o mittenti sono nella blacklist, il messaggio è etichettato come spam, mentre se domini e/o mittenti sono presenti nella whitelist potrebbe non essere necessario eseguire il filtro statistico in quanto il messaggio può essere ritenuto affidabile; il filtro statistico è necessario qualora dominio e/o mittente siano sconosciuti al sistema. Agendo in questo modo si inviano meno messaggi al sistema antispam con conseguente riduzione del suo carico di lavoro.

Invece di avere un'unica coppia di liste SPAM – HAM per sistema, sarebbe molto meglio avere una coppia di liste per utente. Il contenuto delle email può variare pesantemente in base alla tipologia di utenza e di conseguenza si otterrebbe un sistema di filtraggio molto più preciso e mirato se ogni utente avesse la propria coppia di liste. In tal modo risulta anche più difficile per uno spammer aggirare i filtri, in quanto invece di aver a che fare con un solo filtro ha a che fare con n filtri diversi.

5.4 Blocco dello spam a livello del singolo client

Fino a poco tempo fa i client di posta elettronica maggiormente diffusi non avevano al proprio interno dei sistemi antispam: l'utente si doveva creare (e gestire) dei semplici filtri statici che, come descritto precedentemente, alla lunga divengono impegnativi e poco precisi, creando falsi positivi.

Fortunatamente i client di posta attuali includono sistemi antispam più o meno potenti. Vediamo di seguito i principali:

5.4.1 Mozilla ThunderBird

Mozilla ThunderBird è il client di posta elettronica OpenSource più famoso, che assieme al browser FireFox sta facendo concorrenza a Microsoft per quel che riguarda gestione email e websurfing.

ThunderBird include al suo interno un sistema antispam che si basa sui filtri Bayesiani visti precedentemente. Il training iniziale è svolto in automatico dal programma, il quale quando ha qualche dubbio richiede all'utente di contrassegnare il messaggio come spam o come ham, in modo da aggiornare al suo interno la lista delle parole di spam/ham.

Esso include anche un sistema di blocco delle immagini esterne che, come visto precedentemente (Rif. § 3 - "Ottenere conferma degli indirizzi email"), è usato dagli spammer per ottenere conferma dell'indirizzo di posta elettronica della vittima. Tale blocco è attivo per default, ma è possibile disattivarlo per quei mittenti contrassegnati come fidati.

5.4.2 Microsoft Outlook Express

Outlook Express di Microsoft è il client di posta elettronica gratuito integrato in ogni sistema operativo Microsoft insieme al browser Internet Explorer. Esso non include un sistema antispam, e l'unica protezione che offre è quella del blocco delle immagini esterne, attivata di default.

5.4.3 Microsoft Outlook 2003

Microsoft Outlook 2003 è incluso nella suite per ufficio "Office 2003" e propone un approccio che combina blacklist, whitelist e filtri statistici, oltre al già citato blocco delle immagini esterne.

Esso permette di definire blacklist nelle quali possiamo inserire singoli indirizzi email o interi domini (anche di primo livello quali ad esempio .it, .de, .to); se un messaggio combacia con quanto riportato nella blacklist, esso è spostato automaticamente nel folder di "Posta Indesiderata" di Outlook, senza ovviamente passare al filtro statistico.

Le whitelist funzionano nello stesso modo, e vengono automaticamente (se attivato l'apposito flag) popolate coi contatti ai quali scriviamo abitualmente o che sono presenti nella nostra rubrica dei contatti. Anche in questo caso se il mittente combacia con quanto riportato nella whitelist non viene applicato il filtro statistico e quindi la email non viene analizzata. Il filtro statistico di Outlook "dovrebbe" corrispondere ai filtri statistici descritti precedentemente, anche se Microsoft non fornisce informazioni in merito. Stando a quanto riportato su di un documento che descrive le peculiarità di questo servizio, esso è (e viene tuttora) istruito tramite milioni di email sia di spam che di ham, fornite da un apposito team antispam di Microsoft. L'aggiornamento di questo filtro statistico viene fatto mediante il servizio di Windows & Office Update fornito gratuitamente da Microsoft.

6 Altri metodi di Spam

Abbiamo visto sin qui che lo spam è un flagello legato indissolubilmente alla posta elettronica. La definizione di spam però ci porta a considerare come tale anche l'invio di messaggi pubblicitari all'interno di forum e newsgroup, fenomeno che sta prendendo piede ma che con un minimo di accortezza è possibile evitare. Nel seguito sono presi in considerazione tali metodi di spam e le relative soluzioni implementate per limitarne il dilagare.

6.1 Forum

Di forum di discussione ce ne sono parecchi in giro, e senza avere particolari abilità chiunque può aggiungerne uno al proprio sito web. Essi sono molto utili in quanto permettono, come le email, una interazione offline con altri utenti, ed il fatto di appoggiarsi a dei database permette di mantenere online (e quindi consultabile) il loro contenuto per diversi anni. Possono essere considerati (a mio modesto parere) dei veri e propri punti di informazione e se correttamente gestiti possono divenire dei veri e propri punti di riferimento per determinati argomenti.

Proprio per questo motivo sono stati presi di mira dagli spammer che mediante appositi programmi postano messaggi contenenti pubblicità o link a siti web; inondare i forum con messaggi pubblicitari e relativi link permette di ottenere una maggiore visibilità nei motori di ricerca i quali, per determinate parole (come ad esempio "weightloss", "pharmaceuticals", ecc.) proporranno come risultato i siti pubblicizzati nei forum mediante spam.

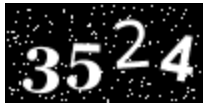
L'inserimento dei messaggi di spam all'interno dei forum avviene per mezzo di appositi spambot, i quali forniscono in automatico le poche informazioni necessarie per postare un messaggio quali il nickname (soprannome), l'indirizzo email ed il messaggio stesso. Siccome quasi tutti i forum tengono traccia anche dell'indirizzo IP dell'utente che ha postato il messaggio, gli spambot provvedono ad inserirne uno finto, sempre per il solito motivo: evitare di essere tracciati.

Per contrastare il fenomeno dello spam molti forum non permettono di postare un messaggio se non si è iscritti, ma anche in questo caso gli spambot fanno tutto in automatico. La maggioranza dei forum si basa infatti su modelli predefiniti che poi vengono mano a mano personalizzati; il fatto di avere una unica base su cui creare tutto il resto permette agli spammer di creare spambot che riescono ad effettuare una registrazione di un utente in maniera corretta su forum differenti che comunque sono basati sul medesimo template. Quindi si può dire che un unico spambot può essere utilizzato per effettuare una registrazione e postare dei messaggi su centinaia (se non migliaia) di forum diversi.

I metodi per arginare questo fenomeno puntano soprattutto sul rendere abbastanza difficile per uno spambot effettuare la registrazione nel forum. Ciò può essere fatto innanzitutto controllando il dominio di provenienza di chi sta effettuando la registrazione utilizzando delle apposite blacklist; in tal modo si può vietare la registrazione da indirizzi IP che sono note fonti di spam.

Altro metodo consiste nell'utilizzo, sempre in fase di registrazione, di **CAPTCHA** ("*Completely Automated Public Turing test to tell Computers and Humans Apart*" - "Test di Turing Pubblico e Completamente Automatico per Distinguere Computer e Umani"), un metodo per verificare se l'utente con cui si sta interagendo è umano oppure si tratta di un bot. Esso consiste in una immagine contenente una sequenza di caratteri alfanumerici che debbono essere inserite dall'utente durante la fase di registrazione; ovviamente per poter proseguire occorre inserire correttamente tale sequenza di lettere, cosa che uno spambot ancora non sa fare.

Esempio 7: CAPTCHA



Nell'esempio viene riportato un CAPTCHA su sfondo nero sporcato con puntini bianchi, con numeri disallineati e scritti con font diversi, in modo da evitare una qualsiasi interpretazione che non sia umana (cioè con software tipo OCR).

Quella innescata tra spammer e CAPTCHA è una lotta in continua evoluzione, dato che anche gli spammer hanno trovato metodi più o meno efficaci per bypassarli. Ad esempio uno spammer che ha un sito web può utilizzare dei CAPTCHA esterni per far entrare gli utenti, e mano a mano che questi inseriscono i valori letti tali valori vanno a popolare un database con tutte le possibili rappresentazioni dei CAPTCHA in modo poi che lo spammer possa provare un attacco a forza bruta sul bersaglio di suo interesse.

In aggiunta al CAPTCHA si può applicare una approvazione della iscrizione da parte dell'amministratore del forum, il quale potrà richiedere alcune righe di commento da parte di chi si vuole iscrivere per poter successivamente concedere o negare l'iscrizione.

6.2 Newsgroup

I newsgroup, o gruppi di discussione, sono praticamente nati insieme ad internet. Si può pensare ad essi come a delle bacheche tematiche, nelle quali ognuno può inserire un nuovo messaggio o rispondere ad un messaggio già presente. Ogni newsgroup riguarda un determinato tema ed al suo interno gli utenti si scambiano opinioni e informazioni, oltre a chiedere magari un semplice aiuto per un qualche problema. Anche essi come i forum possono divenire custodi di moltissime informazioni utili tra le quali cercare, e anche essi come i forum possono divenire bersaglio degli spammer. Gli spammer dei newsgroup inseriscono lo stesso messaggio in diversi newsgroup (effettuano cioè quello che in gergo si chiama "crosspost"), ed il messaggio la maggior parte delle volte consiste di semplice pubblicità con qualche link. Poiché non vi è nessuna forma di controllo e le regole le fanno gli utenti stessi rispettando la "netiquette", l'unico metodo per poter debellare lo spam nei newsgroup consiste nel cancellarli tramite un messaggio di cancellazione.

Un messaggio di cancellazione è un particolare messaggio di controllo formattato in modo tale da richiedere la cancellazione di un determinato articolo dal server delle news ed è ovviamente ad uso esclusivo degli amministratori del newsgroup stesso.

Per decidere quando è ora di eliminare i messaggi di spam all'interno di un newsgroup, viene utilizzato l'indice di Breidbart. Tale indice viene calcolato su di un intervallo di tempo di 45 giorni e nel calcolo si tiene anche conto del numero di newsgroup nei quali il messaggio di spam è stato inserito. Esso infatti è la somma delle radici quadrate del numero di gruppi dove è stata postata una copia del messaggio di spam, moltiplicato per il numero di messaggi inviato al singolo gruppo.

Supponiamo ad esempio che 10 copie del messaggio siano state spedite in 4 gruppi differenti; avremo che l'indice di Breidbart (BI) sarà:

$$[10 \times \text{sqrt}(4)] = 20$$

Ogni gerarchia di newsgroup imposta un proprio valore BI, superato il quale i messaggi di spam vengono cancellati dal news server tramite i messaggi di cancellazione. In questo caso la lotta allo spam viene fatta a posteriori, non potendo implementare una sorta di prevenzione.

7 Statistiche

Stando a quanto riportato da Postini, compagnia americana che fornisce servizi email sicuri, tra giugno e novembre 2006 il numero di messaggi di spam è triplicato, arrivando a definire che nove messaggi su dieci sono spam. La società ha rilevato sette miliardi di messaggi di spam in tutto il mondo nel solo mese di novembre, mentre in giugno tale valore era di "soli" 2.5 miliardi; nella sola Gran Bretagna invece lo spam è aumentato del 50% tra ottobre e novembre 2006.

Stando alle analisi eseguite sembra che la colpa principale di questo incremento sia dovuta alla crescente quantità di Zombie Spam, dovuta al diffondersi di trojan molto complessi sviluppati da programmatori professionisti.

Secondo la società Ipswitch, che fornisce servizi di rete, risulta un incremento dello spam a partire dall'inizio dell'estate scorsa, e gli aumenti coincidono con quanto riportato da Postini, anche se l'analisi di Ipswitch termina ad agosto 2006. Si rileva, infatti, che il 70% di tutte le email è considerato spam, partendo da un 57% di Natale e un 62% nel primo quarto del 2006.

I dati presenti su siti di altre società non sono così distanti da quelli sopra riportati, e tutti indicano che il fenomeno è in costante crescita.

8 Conclusioni

Oltre a creare delle leggi che puniscono chi effettua spam (come recentemente accaduto in America) occorre anche educare i singoli utenti che quotidianamente ricevono spam. Capita spesso sentire i colleghi lamentarsi che ricevono messaggi indesiderati, e poi scopri che cliccano su ogni link che si trova all'interno della email che hanno ricevuto, nemmeno a farlo apposta, da uno sconosciuto. Stesso discorso vale per gli allegati; lo considerano sicuro solamente perché gli è stato spedito da un amico (e ciò mi renderebbe tranquillo se l'amico lavorasse nel campo della sicurezza informatica, ma purtroppo non è così) e quindi si sentono liberi di mandarlo in esecuzione, perché non sanno resistere. Se l'educazione dell'utente è la prima fonte di pericolo per spam e virus, occorre quindi bloccarli prima che giungano al client. Un buon sistema antivirus e un buon sistema antispam configurati correttamente bloccano una altissima percentuale di email indesiderate, ma vi è ancora la remota possibilità che qualcosa sfugga.

Ecco allora che la soluzione principale consiste nella combinazione di tutte le tecniche e tecnologie viste sino ad ora, e quindi:

Il nostro ISP dovrebbe effettuare il blocco delle email spedite da indirizzi IP e domini appartenenti a blacklist; successivamente il nostro server antispam dovrebbe anch'esso effettuare un controllo delle email in entrata mediante blacklist (e whitelist in casi particolari) e successivamente passare le email non bloccate dalla blacklist in un filtro statistico, prima di spedirle al destinatario. Il client di posta del destinatario deve avere attivo per default il blocco del download delle immagini esterne, oltre a contenere una blacklist creata dall'utente stesso. Tutto ciò solamente per lo spam, ma è chiaro che lo stesso comportamento deve essere tenuto coi virus e i trojan, tramite i quali si propagano gli spambot et similia. Come ultima cosa, l'utente finale deve essere istruito su come comportarsi in caso riceva una email sospetta, e sapere che può contare su un supporto che saprà dirgli cosa fare, e deve essere consapevole del tipo di danni che può creare se certi argomenti vengono affrontati con troppa leggerezza.

GLOSSARIO

HAM: Messaggio di posta che non è spam = messaggio lecito.
UCE: Unsolicited Commercial Email, altro termine per identificare lo spam.
UBE: Unsolicited Bulk Email, altro termine per identificare lo spam.
ORDB: OpenRelay DataBase, database di server open-relay.

ⁱ http://www.mail-abuse.com/spam_def.html

ⁱⁱ <http://www.networkworld.com/research/2001/0910feat.html>