Giovedì, 22 maggio 2014

Spam – Stay Out of the Spam Folder

Email marketing is a preferred marketing method among small businesses, eCommerce companies, entrepreneurs and marketing specialists in the current technological age. It provides a way to reach an abundance of established and potential customers efficiently. Even more so, it allows business professionals to regain lost customers/clients.
In many ways, email marketing campaigns are a certain path to gain exposure, sales, profits and additional success. Unfortunately, many marketers have inadvertently turned a marketing gold mine into a missed opportunity. The reason is often the result of being flagged by email providers as “spam”, or having individuals categorize your company newsletters as spam.

Does Your Email Marketing Campaign Mimic Spam?

If your email marketing campaign is in violation of the CAN-SPAM Act of 2003, your newsletters will more than likely be marked as Spam. In order to prevent noncompliance, you’ll need to set in place, and follow, a specific email policy. All company email correspondence must offer an opt-out link. Additionally, newsletters should be sent in appropriately spaced time intervals. It is recommended to send one per week at the most, and every other week is even better.

Cleaning Up Your Newsletters

A few simple guidelines can ensure that your newsletters bypass the spam folder all together, thereby remaining in the inbox where they may eventually be read. Include a catchy title, which is clear with intent. In other words, you want your title to catch the attention of the intended reader. However, you also want them to know exactly what is contained within the email newsletter through the title. Be sure to avoid spam text-based identifiers, such as free, claim, immediately, act now, or don’t miss, as these are often identified by email providers as spam.

Providing a Value to Your Email List

Beyond all the technical do’s and don’ts, the best way to prevent being thrown into the spam box, is to provide your newsletter recipients with some form of value. This could be an intriguing story that’s currently trending, a quality article that’s filled with tips or valuable instructions. You can also simply insert a fun article that adds entertainment value. After crafting your newsletter, take a moment to read it. If it’s not valuable to you, then more than likely the recipients of your newsletter won’t find any value either.

The Bottom Line

To avoid spam filters and manual spam marking, don’t over email your contact list. You’ll also want to make sure that you always include an opt-out link. Additionally, you need to avoid spam identifier words. Finally, and possibly the most important, create smart titles that open up to a valuable newsletter. That’s the bottom line to staying out of the spam folder.

Scritto da Raimondo Fanale in Email marketing, Spam at 09:56

Lunedì, 7 maggio 2007

nuova ondata di phishing

UPDATE del 08/05/2007a danno di Poste Italiane. Questa volta oltre che segnalare alle Poste Italiane il problema, pubblico anche sul mio blog l'email ricevuta.Con un po' di attenzione si capisce bene che l'email è un falso. Il vero problema è che ormai quasi tutti gli utenti hanno un atteggiamento pigro e svogliato durante la lettura di documenti elettronici in genere, e non solo della posta, quindi spesso sono tratti in inganno dalla distrazione e non tanto dalla mancanza di capacità.

questa è l'email ricevuta da poco. Ci sono vari elementi identificativi.differenze nello stile della formattazioneitaliano approssimativomancanza di lettere accentate, probabilmente dovuta ad una errata interpretazione del charset da parte del software di inviole note legali : "2007 Banco Poste
Italiane . Tutti i diritti hanno riservato"l'indirizzo cui ci si collega non è quello di poste italiane, ma un ip numerico con la pagina incriminata: http://211.23.204.19/.www.poste.it/index.htmnon ho un account su Poste Italiane.Per un approfondimento sul phishing, consiglio la pagina di WikiPediaUPDATE: mi hanno sospeso il conto bancoposta...ed ovviamente è un falso anche questo perchè non ho un account bancoposta. Ma stavolta ho voluto approfondire ed "assecondare" questa email. quindi ingorando ogni buona norma ed ogni avvertimento del mio browser (messaggio: "sito contraffatto", su firefox), ho messo nome utente e password richiesti, ovviamente inventati: ppp/ppp .Ecco la schermata che mi si presenta, dove mi chiedono di inserire il codice di sicurezza (dispositivo) del mio conto per verificare la mia identità:ok, notare che la url mostrata dal mio browser è http://mconway827.com.p11.hostingprod.com/store/confirmbancoposta.php.htm che onestamente poco ha a che fare con le Poste Italiane. Come primo tentativo ho chiesto di proseguire senza inserire il codice di sicurezza. E la pagina non ha dato segni di vita ed è andata in loop. Inserendo un codice inventato (per sicurezza ho utilizzato caratteri accentati) la pagina ha inviato i dati e mi ha rediretto sulla vera home page di Poste Italiane... dove tra l'altro esiste un link sulla destra dove si avvertono gli utenti di stare attenti al phishig. L'indirizzo è questo: avvertimento anti-phishing di Poste Italiane Dove spicca in risalto la dichiarazione che Poste Italiane non chiede mai, attraverso messaggi di posta elettronica, di fornire il "nome utente", la password, il codice
per le operazioni dispositive di BancoPosta online, i dati delle carte
di credito o della carta Postepay.

Un invito alla prudenza ...

Scritto da Raimondo Fanale in Spam at 07:30

Domenica, 6 maggio 2007

preoccupazione dalla Polonia

Se da un lato ci sono i problemi degli utenti con lo spam, dall'altro ci sono le preoccupazioni e la pressione delle ditte e delle compagnie di telecomunicazioni.I dati stimano perdite annuali di produttività e di denaro elevatissime, eppure la piaga dello spam non viene eliminata. Vediamo cosa succede in Polonia.A maggio la Polonia è riuscita a segnare un nuovo record portando al 5% il livello di spam che fuoriesce dai server di tpnet.pl (Polish Telecom o Telekomunikacja Polska) .

Si tratta del 5% dello spam mondiale, che lascia la Polonia nella top-ten delle nazioni con il più alto tasso di spam attivo al mondo, ovvero una delle nazioni/reti che generano più spam.La preoccupazioni delle ditte polacche non è solo basata sulla noiosissima e fastidiosissima pioggia di email indesiderate che ricevono, ma sui mancati guadagni dovuti al fatto che non riescono più ad inviare email ai loro contatti esteri, che applicano filtri leggermente più avanzati, o che si basano sulle black list.Anche considerando che tpnet ad oggi ha circa 300 ip in blacklist non abbiamo forse la misura del problema. Ma se invece consideriamo che la maggior parte dello spam usa tpnet come relay verso il resto del mondo a causa di scarsi investimenti sulle attività di sistemistica e sicurezza informatica, forse il problema diventa più comprensibile.Diventa più comprensibile anche se aggiungiamo un altro tassello: le connessioni wireless della stessa tpnet non sono protette.E' un problema economico o culturale? Direi entrambi, perchè se da un lato c'è la compagnia telefonica che non investe nel settore security, dall'altro ci sono gli utenti che di fatto chiedono costi di accesso sempre più bassi e sono i primi a non preoccuparsi di come deve essere utilizzata e mantenuta un connessione wireless.Fino a quando il cane continuerà a mordersi la coda?

Scritto da Raimondo Fanale in Spam at 23:21

Sabato, 5 maggio 2007

perchè lo spam aumenta

Altro piccolo promemoria sull'argomento dopo l'uscita di un post da parte di Yazan Gable, ricercatore della Symantec , ed altre security firms.In questo modo spero anche di spiegare e tenere a mente perchè l'interesse delle aziende che si occupano di sicurezza informatica e di gestione delle reti si sono concentrate sullo spam, mentre sempre più raramente si sente parlare di attacchi DDOS (Distributed Denial of Service).
Negli anni passati uno dei problemi più grandi per chi si occupa di gestione di una rete o di sistemi di prevenzione dei danni e disservizi erano i DDOS.Ora le cose sono cambiate, anche a causa di un processo di gestione economica.

Analizzando il problema del dDOS si intuisce che istallare e mantenere dei pc zombies è una attività onerosa anche per chi la pratica e non solo per chi si deve occupare della loro "disinfezione". Considerando che finanziare una attività di questo tipo ha costi alti anche per il committente, c'è stato quindi uno shift verso attività meno costose e più lucrose, come quello dell'invio di email indesiderate.Inoltre spesso non c'è nessun vantaggio economico nel tenere un server giù per ore o giorni, soprattutto se lo stesso pc, server o rete possono essere sfruttati come veicolo per relay dello spam.Come relay dello spam intendo anche la semplice consegna di tonnellate di email direttamente al server di arrivo e non le tecniche più sofisticate di bouncing che sfruttano le stesse RFC della posta elettronica.Spero sinceramente che questa brevissima considerazione sullo stato di determinate attività informatiche possa essere utile a tutti quelli che si impegnano nel mantenere pulita la rete aziendale.Via: theregister

Scritto da Raimondo Fanale in Spam at 09:35

Giovedì, 3 maggio 2007

promemoria sullo spam

Pubblico questo post come promemoria personale di un ragionamento che sto facendo da diversi mesi con il mio amico Sante e con la consulenza di MonjaEntrambi ci troviamo di fronte ad un problema enorme con i servizi web che offriamo ai nostri clienti ed in particolare si tratta ancora dell'annoso problema dello spam. Io cerco di continuare i miei studi sul campo e di applicare diverse teorie e soluzioni ma sono arrivato a diverse conclusioni:non si possono applicare filtri troppo restrittivimolti dei software attualmente in commercio non sono risolutivi o richiedono troppa manutenzione o l'intervento dello stesso utente nessuna delle due conclusioni, ovviamente, mi soddisfa.

La prima: noi, come altri providers, offriamo servizi ai nostri clienti. Applicare regole di filtro troppo restrittive può causare la perdita di email. La nostra fortuna è che con i nostri clienti abbiamo un buon rapporto e dialogo continuo, quindi riusciamo, bene o male, a seguire e mediare le esigenze di ognuno.La seconda: i software attualmente in commercio prevedono l'assoluto intervento dell'utente, che invece spesso è pigro nello svolgimento di attività che in fondo non sono di sua competenza.Tali software, se non seguiti o gestiti nel tempo non sono risolutivi e servono ad eliminare ben troppo poca posta indesiderata.Soluzioni non gestite sono quindi risolutive quando il livello di spam si aggira intorno al 15% dell'intera posta. Ad oggi ci troviamo, invece, davanti al dato reale che l'85% della posta è spam, e diventerà il 90% entro fine anno. Questo vorrebbe dire eliminare 9 email su 10... e la cosa, mi scuso per la frase, mi sembra francamente una grandissima stupidaggine.Ora, ci sono diversi sistemi per la gestione del problema, e mettendo da parte quelle che sono le mode o le pubblicità che spesso si trovano in giro per la rete nessuna è davvero risolutiva. Al momento personalmente utilizzo 4 sistemi diversi per la gestione dello spam, ma il tutto sta diventando troppo oneroso in termini di gestione e manutenzione sistemistica. Fortunatamente lo spam non è ancora così cambiato da dover azzerare il lavoro di anni e con l'aiuto di filtri Bayesiani, algoritmi Markoviani, whitelists, il tutto che lavora su dati raccolti su un campione di circa 10 milioni di email transitate nel corso del tempo, più circa 50milioni di spam comunque non gettate, ma filtrate ed elaborate da software interni il costo di manutenzione dei prossimi due anni dovrebbe scendere di circa il 50%. Come dicevo, questo è solo un promemoria personale, quindi fatemi in bocca al lupo

Scritto da Raimondo Fanale in Spam at 15:16

Lunedì, 12 febbraio 2007

la statistica, lo spam e i falsi positivi

Un paio di clienti, preso il coraggio a due mani, mi hanno chiesto che cosa intendessi con "falso positivo" quando gli spiegavo che la manutenzione di un server di posta non è una cosa da ridere.Sono previste attività di controllo molto serie ed onerose.Allora, dopo tutti i discorsi fatti sulla statistica e gli algoritmi di verifica e controllo delle email , mi è venuto i mente di spiegare la cosa facendo un paragone con le liste di volo.Metti di essere la moglie del Senatore Ted Stevens (Alaska) e di chiamarti Cat Stevens (esatto!!! proprio come il cantante...). Ti presenti all'imbarco, dopo aver pagato il biglietto, e ti dicono che non puoi viaggiare per motivi di sicurezza.Ecco che il tuo ego viene solleticato e cominci a farti i films più assurdi del tipo "allora vuol dire che su questo volo ci sono o potrebbero esserci prolemi e quindi qualcuno controlla che io sia al sicuro, d'altra parte sono la moglie di un senatore!!!!"Invece scopri che non puoi viaggiare in aereo a causa delle liste di no-fly compilate dal governo, e che la motivazione per cui ti trovi in quella lista è che Cat Stevens (il cantante) essendo musulmano (si chiama Yusuf Islam) è stato incluso nelle liste di no-fly per prevenire attacchi terroristici. Ecco, questo è un falso positivo.Può succedere anche alle tue email di essere oggetto di falsi positivi dovuti ad una taratura errata dei filtri antispam.

Scritto da Raimondo Fanale in Spam at 12:05

multe agli spammer

anche se è una notizia vecchia, voglio riportarla per dare una speranza a chi di spam soffre e a chi lo spam lo combatte ogni giorno.il 2 febbraio 2007 l'OPTA (http://opta.nl/asp/en/) ha elevato un multozzo ad uno spammer. Cosa faceva il tipo? le solite cosette: invio di spam su pillole per aiutare la virilità, uso di proxy per l'anonimato. La multa è stata di 75.000 eurini per aver inviato:9 miliardi di email (loro parlano al solito di billion)guadagno minimo stimato di 52.000 dollariuso di proxies per celare la propria identitàtra i proxies usati c'erano anche computers di ignari utentiL'aiuto viene dalla Microsoft, che pare abbia fornito informazioni rilevanti per l'identificazioned degli spammers..Per chi volesse leggere l'articolo completo: http://opta.nl/asp/en/newsandpublications/pressreleases/document.asp?id=2126Ora la questione solleva due interrogativi:lo spammer ha inviato una quantità stimata di 9 miliardi di email, pare usando anche pc di utenti ignari. Ma la pirateria informatica non è anche un reato più grosso dello spam?Seconda questioneForse la Microsoft cerca di farsi amici i governi e l'opinione pubblica attraverso queste iniziative?

Scritto da Raimondo Fanale in Spam at 00:41

Mercoledì, 17 gennaio 2007

wordpress e lo spam - 2a parte

Impegnato a fare un po' di traduzioni di software proveniente da Corea e Romania, eccomi di nuovo sul tema Worpdress e lo spam. Ho letto attentamente quanto scritto da Napolux ad inizio mese e le risposte che sono arrivate. Io personalmente non sono favorevole ad operazioni di questo tipo. Rinominare un file di un software che non stai sviluppando ti obbligherà sempre a fare questa operazione a vita. Ovvero ti "uccidi" con il versioning. Il trucco suggerito da Naploux è bello, semplice e funzionale (lo dico perchè sono verametne convinto che possa funzionare) ma per chi deve costantemente aggiornare il WordPress è un lavoro in più. Personalmente preferisco lavorare su .htaccess e bloccare l'accesso diretto al file. Per chi non lo conoscesse, quindi, consiglio questo plugin creato nel 2005. Per chi non volesse istallare il plugin spiego cosa fa: inserisce una riga nel file .htaccess del tipo
RewriteRule ^wp-trackback\.php.*$ - [F,L]\n
Una semplice riga da poter replicare come si vuole e per qualsiasi file. La riga riportata blocca l'accesso diretto ai trackback, ma può essere modificata per il file wp-comment .ATTENZIONE. la riga suggerita è abbastanza "generica"" ma ovviamente potrebbero essere necessarie delle modifiche ad hoc per adattarsi al tuo file .htaccess .

Scritto da Raimondo Fanale in Software per blog, Spam at 15:09

Domenica, 31 dicembre 2006

lo spam cambia - un omaggio a ordb

Un saluto gioioso di fine anno a tutti. Un saluto nostalgico e grato al team di ORDB, e al loro sito. Per chi non lo conoscesse, ORDB è un servizio di blacklist basato sulla verifica degli open realy mail server (in breve: si proponeva di combattere lo spam). Per anni ci ha aiutato e ci ha accompagnato nelle nostre vite informatiche, senza che spesso ci accorgessimo della sua esistenza. E' per questo che sento di dover ringraziare pubblicamente tutto lo staff e tutti i volontari di ORDB per il lavoro svolto negli anni. Purtroppo lo spam ed i metodi utilizzati dagli spammers sono cambiati ed un servizio come ORDB rimane valido solo parzialmente. Lo stesso staff invita a considerare nuovi metodi di antispam, come il greylisting e l'utilizzo di filtri su contenuti. Riporto le loro parole:
We encourage system owners to remove ORDB checks from their mailers
immediately and start investigating alternative methods of spam
filtering. We recommend a combination involving greylisting and
content-based analysis (such as the dspam project, bmf or Spam Assassin).Il 18 dicembre ha segnato la fine del loro servizo, il 31 dicembre 2006 segna la fine e la scomparsa del loro sito. Grazie ancora.Per chi volesse sapere come era ORDB pubblicherò a breve nell'area downloads delle stampe in pdf, a memoria del loro sforzo.Passiamo ora a cose meno romantiche, e pubblico di seguito le alcune ultime statistiche proposte sullo spam.

Spamhaus ci propone la statistica giornaliera dei dieci "migliori" spammers , suddivisi per nazionireti di ISP ROKSO (Register Of Known Spam Operations)Sono statistiche che vengono aggiornate giornalmente, quindi pubblico lo screenshot delle statistiche del 31 dicembre relative al 30, sperando di essere abbastanza sveglio domani per pubblicare anche lo screenshot del 1 gennaio 2007 relativo ad oggi...

Scritto da Raimondo Fanale in Spam at 12:44

Martedì, 12 dicembre 2006

La più bella immagine di spam che ho ricevuto

Chi legge un pochino il mio blog saprà che sto conducendo una battaglia personale contro lo spam, e poco tempo fa parlavo dello spam di tipo image-based.Allora voglio inaugurare una nuova categoria sul mio blog che parla appunto dello spam.Dopo anche i commenti di napolux al mio post ho messo su un paio di soluzioni (ad esempio per controllare il crc delle immagini) che mi sembravano carine... allora è cominciata una vera e propria guerra tra me e LORO!!!Ecco l'ultima che mi è arrivata...

Scritto da Raimondo Fanale in Spam at 11:20

Lunedì, 13 novembre 2006

image-based spam

UPDATE del 15-11-2006Chiedo scusa perchè sto scrivendo un nuovo post sullo spam. Forse qualcuno si annoierà, ma se davvero la funzione dei blog è quella del "tam-tam" delle informazioni, allora sono contento di dare e di ricevere.Mi sto scontrando con un problema serio sullo spam, ed in particolare una forma di esso: l'image-based spam.Racconto una favoletta: c'era una volta "lo spammer". Dava fastidio, anche perchè con i bei modem a 2400 baud anche 1 solo matrix indesiderato portava a pronunciare imprecazioni e maledizioni verso il suo autore.
Poi lo spammer ha avuto fortuna, ed ha deciso che era cosa buona e giusta diffondere il suo verbo, ed internet è diventata la sua terra. Poco importa se chi riceve posta non ha nessuna intenzione di ricevere informazioni non desiderate. Poco importa se riceve le stesse informazioni da 10 fonti diverse e 10 volte al giorno. Poco importano le leggi e i filtri. Lo spammer è convinto del suo verbo. E trova sempre metodi migliori. Già diversi anni fa arrivavano le prime email di spam image-based dalla... non so se dire "Russia con amore" o "dalla Russia con furore" (e qui chiedo venia per la commistione di citazioni...)In sostanza si tratta di questo: vere e proprie immagini che contengono il testo del messaggio pubblicitario indesiderato. Generlamente nessun'altra informazione.Cambiano i testi, cambiano le dimensioni, cambiano i colori. Le stesse dimensioni dell'immagine sono spesso studiate per ingannare i filtri, e sono degne di una menzione al merito per l'usabilità: sono leggibii a varie risoluzioni e con tutti i mailers. A volte contengono dei leggeri disturbi per renderne ancora più difficile l'individuazione. Mantengono solo un punto comune: sono email indirizzate a più indirizzi contemporaneamente. E' un punto di partenza, non di arrivo...Ed ora come al solito un po' di dati: da marzo la stima di crescita di questo tipo di spam è del 300%. Da giugno 2005 a giugno 2006 la percentuale di questa forma di spam è salita dall'1% dello spam mondiale al 12% (vedi qui un interessante articolo, anche se datato...).Inoltre per i providers è molto dannoso: maggiore banda consumata (un email di spam testuale ha il peso medio di 5,5kb, una image-based di 18kb) e maggiore potenza di calcolo sui servers per impostare dei filtri su immagini.UPDATE: per chi legge l'inglese, qui trovate altri riferimenti interessanti.

Scritto da Raimondo Fanale in Generale, Spam at 22:36

Giovedì, 9 novembre 2006

qualche dato sullo spam via email

tutti ne parlano e tutti lo odiano. Ci sono diversi modo di considerare lo spam che arriva via email: quello tecnico, quello sociale, quello economico...A noi in questo momento interessa quello (poco)tecnico/statistico.Mi piacerebbe condividere qualche dato preso da uno dei server che controllo giornalmente.
I dati si riferiscono a ieri (08/11/2006), arco temporale di 24 oreQuantitàMotivazione%4Recipient address rejected0,0035Other0,00424Local access rule: Sender address rejected0,0191448Relay access denied1,1594840Bad HELO3,8736159Sender Domain not found4,92812162RBL list.dsbl.org9,73122907User unknown18,32929685RBL sbl-xbl.spamhaus.org23,75247744RBL bl.spamcop.net38,202totale124.978email di spam solo su un server in un giorno100%
Cosa vogliono dire questi dati? Quelli più importanti, secondo me, sono quelli relativi agli errori su HELO e su Sender Domain not Found.Spiego subito qual'è la motivazione che mi spinge a dire che sono i più interessanti.Gli errori su HELO.Sono generati da mail servers che si presentano in modo strano o non corretto. Ce ne sono molti che si presentano con nomi non conformi alle RFC, del tipo e il nomedi uno script cgi (ad esempio...) che generano un errore proprio sul tipo di nome con il quale si presentano. Poi ci sono (ad esempio)che vengono rigettati a causa del fatto che non sono hostnames qualificati. , infatti, non mi risulta essere associato a nessun host conosciuto, neanche interno alla rete. Il , invece, può essere generato da programmi di spam che tentano una via per fare relay. Il vero problema è che tutte queste casistiche hanno le loro eccezioni: potrebbe essere un nome di un server realmente esistente, il cui sistemista non ha provveduto ad associare un vero e proprio hostname e nessun reverse name. Oppure è un server interno di un ufficio o una azienda che non ha la possibilità tecnica di configurare un hostname (non scandalizzarti... molti fornitori di connettività "storcono il naso" anche se si chiede un dominio di terzo livello, figuriamoci un hostname e un reverse associati al proprio ip...) potrebbe ricadere nello stesso caso di , oppure essere l'esperimento di qualche sistemista Gli errori Sender Domain not found.Generalmente faccio controllare al mail server o al mail gateway che il dominio che spedisce sia realmente esistente. Quando non lo è arriva questo tipo di errore. Ecco i contro:il dominio che spedisce o il dns che lo risolve potrebbero essere temporaneamente "fuori uso", quindi si rischia di rigettare una email buona. Per questo motivo la regola non deve essere ferrea, ma flessibile e dovrebbe permettere all'MTA di fare altre verifiche nelle ore successive alla ricezione di questo tipodi email.il dominio che spedisce riestra nei casi di mancata impostazione dell' hostname e/o del reversePer finire.Se vuoi avere un'idea di come va lo spam nel mondo puoi collegarti a questi due indirizzi:statistiche spamhausstatistiche senderbase

Scritto da Raimondo Fanale in Software per server, Spam at 17:20

Mercoledì, 16 agosto 2006

DSPAM - antispam software

Dspam è un software per il filtraggio della posta indesiderata, il cosiddetto SPAM, scalabile, open source e pensato per essere utilizzato negli ambiti più diversi, dal mailer all'MTA. La sua efficacia è ormai testata a vari livelli, ed io stesso lo implemento sui miei server di posta o sui server di posta che installo per i miei clienti.
Le sue caratteristiche essenziali sono:open source, rilasciato con licenza GPLdimensioni ridotte (l'attuale pacchetto di installazione "pesa" solo 726kb)filtraggio dal 99.5% al 99.95% della posta indesiderata (e vi assicuro che se ben gestito questi numeri sono reali)ottima velocità di filtraggio anche in combinazione con più filtri (ad esempio antivirus)motore probabilistico ed utilizzo di vari algoritmi di autoapprendimento introduzione di algoritmi e engine di tipo Concept Identification, Neural Networking, Message Inoculation , de-obfuscation, Bayesian Noise Reduction scritto interamente in C per questioni di performancesupporto per vari metodi di memorizzazione: SQLite, Berkeley DB, MySQL, PostgreSQL, Oracle, e un hash driver proprietariosupporto per MTA come Sendmail, Postfix, Qmail, Courier, ed Exim.Il suo funzionamento prevede modalità server o tramite libreria, ed è quest'ultima (la libdspam) che viene usata come base per la scrittura di molti plugin per mailer come ad esempio il mozilla thunderbird.In realtà ci sono dei contro : l'interfaccia non prevede un facile sistema di localizzazione, ovvero per supportare sistemi multilingua bisognerebbe riscriverla da zeroil suo uso a livello server ha causato una "dimenticanza" nell'implementare plugin di gestione all'interno di webmails. Ovviamente ognuno può scrivere il proprio Questi due soli punti a sfavore ne fanno di fatto un software poco gestibile a livello utente, dal momento che la sua interfaccia non si presenta davvero user-friendly

Scritto da Raimondo Fanale in Software per server, Spam at 22:36