# *Lo SPAM nella Posta Elettronica*

*Cos'e` e come ci si puo` difendere*

***Caffe` te(le)matico del 4 Ottobre 2004***

**Servizio Calcolo e Reti Sez. INFN Torino**

***Alberto D'Ambrosio***

# *Etimologia…*

**ULTERIORI INFORMAZIONI...**

**http://www.spam.com/**

# Spot..

# *Terminologia…*

- **UCE**: Unsolicited Commercial Email
- **UBE**: Unsolicited Bulk Email
- **spam**: Le Email che gli utenti non sono interessati a ricevere
- **ham**: Le Email *buone* (nel senso di *non-spam*)
- **falsi positivi**: Email di tipo *ham* identificate come *spam*
- **falsi negativi**: *Spam* non identificato dall'anti-spam

**ULTERIORI INFORMAZIONI...**

**http://spam.abuse.net/**

# *MTA*

BSD (Berkeley System Distribution) Sendmail e` un Mail Transport Agent (MTA). Questo vuol dire che il suo compito e` quello di trasportare la posta elettronica dalla sorgente alla destinazione, possibilmente fungendo da gateway tra protocolli diversi di spedizione delle Email, trasformando gli indirizzi di posta e instradando le Email secondo opportuni criteri.

Sendmail (almeno nella sua funzione di MTA) non e` vincolato ad alcun protocollo di formato o di trasporto specifico, il suo compito e` solamente quello di instradare i messaggi di posta, in base alle disposizioni date nel file di configurazione.

**ULTERIORI INFORMAZIONI...**

http://www.sendmail.org/

# *MILTER*

Interfaccia che consente di utilizzare Sw esterno (filtri) agli MTA (Sendmail) per validare o modificare i messaggi mentre transitano attraverso lo stesso MTA.

Viene normalmente utilizzata come interfaccia efficiente (sicura, affidabile, ad alte prestazioni) con anti-virus, anti-spam e content-scanner.

Non risulta presente in tutti i MTA; ad esempio, lo e' in Sendmail, ma non in Postfix.

**ULTERIORI INFORMAZIONI...**

http://www.milter.org/

http://www.milter.info/

# MUA

Sendmail non viene utilizzato direttamente dall'utente finale. Ad esso infatti vanno affiancati i MUA.

I Mail User Agents sono quei programmi che costituiscono l'interfaccia dell‘utente a Sendmail (o ad altri sistemi di trasporto) tramite i quali si possono comporre e passare Email ai MTA . Questi programmi (esempio: pine, netscape) formattano l'input dell'utente e lo passano a Sendmail (in spedizione) e prelevano i nuovi mail da un'area di spool (in ricezione).

**ULTERIORI INFORMAZIONI...**

http://www.washington.edu/pine/

http://www.netscape.com/

# *LDA*

Sendmail non si occupa di effettuare la consegna finale delle Email. Di questo si occupano i LDA.

I Local Delivery Agents sono quei programmi tramite i quali le Email passano dai MTA ad un'area di spool (*INBOX*).

Alcuni di questi programmi (esempio: procmail) hanno funzionalita` piu` ampie e possono cosi essere utilizzati per filtrare, catalogare, smistare, ecc.. i messaggi al momento della consegna.

**ULTERIORI INFORMAZIONI...**

http://www.procmail.org/

# *La Netiquette…*

**Con lo SPAM si ha:**

- **violazione delle norme di Netiquette in vigore in Italia**
- **violazione dei principi di uso corretto delle risorse di rete enunciati nel documento RFC1855 (Netiquette Guidelines)**
- **(probabile) violazione del C.P.**

**ULTERIORI INFORMAZIONI...**

**http://www.to.infn.it/servizi/calcolo/netiq-ita.html**

**http://www.rfc-editor.org/rfc/rfc1855.txt**

# *La prevenzione…*

- Pubblicizzare il meno possibile il proprio indirizzo Email
- Non rispondere con Email di protesta ai messaggi di SPAM
- Non acquistare merce pubblicizzata tramite SPAM
- Non spedire Email in formato HTML

**ULTERIORI INFORMAZIONI...**

**http://www.to.infn.it/servizi/calcolo/spam-ita.html**

# *Le armi a disposizione… (1)*

**Spamassassin (2.64):**

- **Serie di test euristici con algoritmi genetici**
- **Correttore statistico Bayesiano**
- **Client DCC**
- **Client RAZOR**
- **Client PYZOR**

**ULTERIORI INFORMAZIONI...**

**http://www.to.infn.it/servizi/calcolo/spam-ita.html**
**http://www-ccrma.stanford.edu/~jos/bayes/Bayesian_Parameter_Estimation.html**
**http://www.niedermayer.ca/papers/bayesian/bayes.html**

# *Le armi a disposizione… (2)*

**Server Nazionale DCC (Distributed Checksum Clearinghouse):**

- **dcc.to.infn.it**
- **Primo (unico..) server Nazionale INFN (Secondo in Italia)**
- **Appartiene alla rete mondiale di oltre 250 server**
- **Realizzato nell'ambito di un gruppo di lavoro GARR**
- **Per la Sez. INFN di Torino il vantaggio del server "in casa"!**

**ULTERIORI INFORMAZIONI...**

**http://www.rhyolite.com/anti-spam/dcc/**

# *Le armi a disposizione… (3)*

**Sendmail 8.13.1 con FEATURE *'greet_pause'*:**

- **Viene rifiutata la connessione con gli host che non rispettano l'handshake iniziale del protocollo SMTP**
- **Aumento della protezione verso *SMTP slammers***
- **Diminuzione del 20-30% dello SPAM**

**ULTERIORI INFORMAZIONI...**

**http://www.sendmail.org/8.13.0.html#RS**

**http://www.sendmail.org/8.13.1.html#RS**

# *Le armi a disposizione… (4)*

**Protezione contro i VIRUS:**

- **Content-scanner: AMaViS (amavisd-new 2.1.1)**
- **Anti-virus: Sophos 3.85**
- **Attachment-renaming: vbsfilter 1.7**

**Il content-scanner effettua una scansione della singola Email e ne controlla il contenuto tramite l'anti-virus.**

- **INFETTA: Non consegnata. Messa in quarantena. Notifica al destinatario.**
- **SANA: Attachment rinominato. Consegnata al destinatario.**

**ULTERIORI INFORMAZIONI...**

**http://www.ijs.si/software/amavisd/**

**http://www.sophos.it/**

**http//aeschi.ch.eu.org/milter/**

# *Quindi, abbiamo vinto?*

***NO!***

- **Alta % di personale impegnato**
- **Alta % di CPU/RAM dedicata**

**Quindi, per bene che vada, la situazione “costa”.**

# *Cosa bolle in pentola…*

- Passaggio alla nuova generazione (ASF) di SpamAssassin
- Possibilita` di (parziale) centralizzazione dello SpamAssassin:
  - Attuale default: disabilitato, l'utente se lo attiva da solo
  - Futuro default: abilitato, l'utente ne chiede la disattivazione
- Possibilita` (facoltativa, <u>su espressa richiesta degli utenti</u>) di rifiutare le Email individuate come SPAM dallo SpamAssassin
  - Pro: eliminazione del folder contenente lo SPAM da controllare
  - Contro: il rifiuto riguarderebbe anche i Falsi Positivi

**ULTERIORI INFORMAZIONI...**

http://spamassassin.apache.org/

http://www.ijs.si/software/amavisd/#faq-spam

# …tra mille difficolta'!

- Hw non sempre sufficiente: andrebbe aggiunta ulteriore CPU…
- Ciclo di vita del Sw brevissimo!
- Inesistenza di conoscenze consolidate
- Inesistenza di Corsi standard in materia
- Unici due corsi (annuali) in USA:
  - LISA'04, Atlanta
  - ApacheCon 2004, Las Vegas
- Corsi attualmente non frequentabili da personale INFN
- Impegno personale elevatissimo
- Rischio di abbassamento del livello di (alta) qualita` del Servizio di Posta Elettronica della Sez. INFN di Torino a quello medio delle altre Sezioni

**ULTERIORI INFORMAZIONI...**

http://www.usenix.org/events/lisa04/

http://www.apachecon.com/2004/US/

# *The End..*

**Centro di Calcolo INFN - Torino**

***Alberto D'Ambrosio – 4 Ottobre 2004***

***Alberto.Dambrosio@to.infn.it***