Gruppo *sec-mail* : status report

Roberto Cecchini

GARR_05

Pisa, 12 Maggio 2005

I membri attivi

- Enrico Ardizzoni (Università di Ferrara)
- Alberto D'Ambrosio (INFN, Torino)
- Roberto Cecchini (INFN, Firenze)
- Fulvia Costa (INFN, Padova)
- Giacomo Fazio (INAF, Palermo)
- Antonio Forte (INFN, Roma 1)
- Matteo Genghini (IASF, Bologna)
- Michele Michelotto (INFN, Padova)
- Ombretta Pinazza (INFN, Bologna)
- Alessandro Spanu (INFN, Roma 1)
- Alfonso Sparano (Università di Salerno)

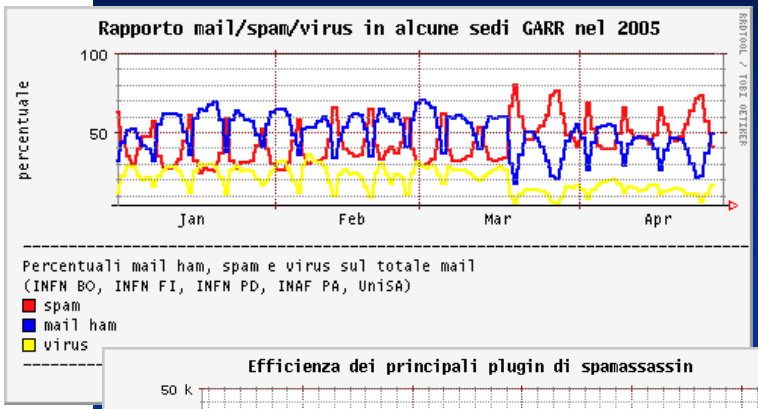
Scopi

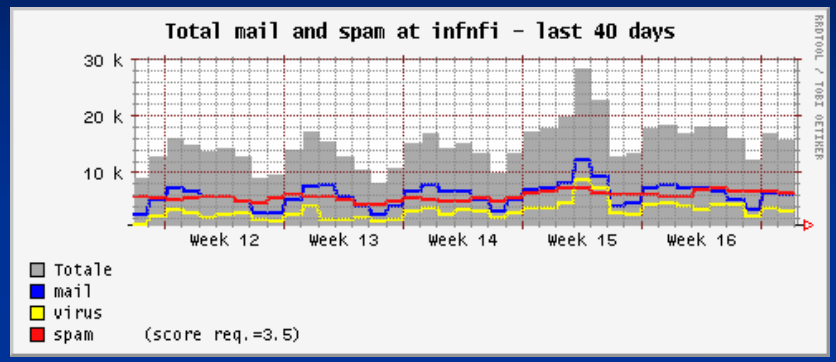
- Metodologie anti-spam e anti-virus
- Stesura di “best practices” per la configurazione dei servizi di posta e la protezione dei mail server;
- Metodologie di autenticazione del mittente.
- Sito web: http://www.garr.it/WG/sec-mail
- Informazioni sul gruppo: <secmail-info@garr.it>

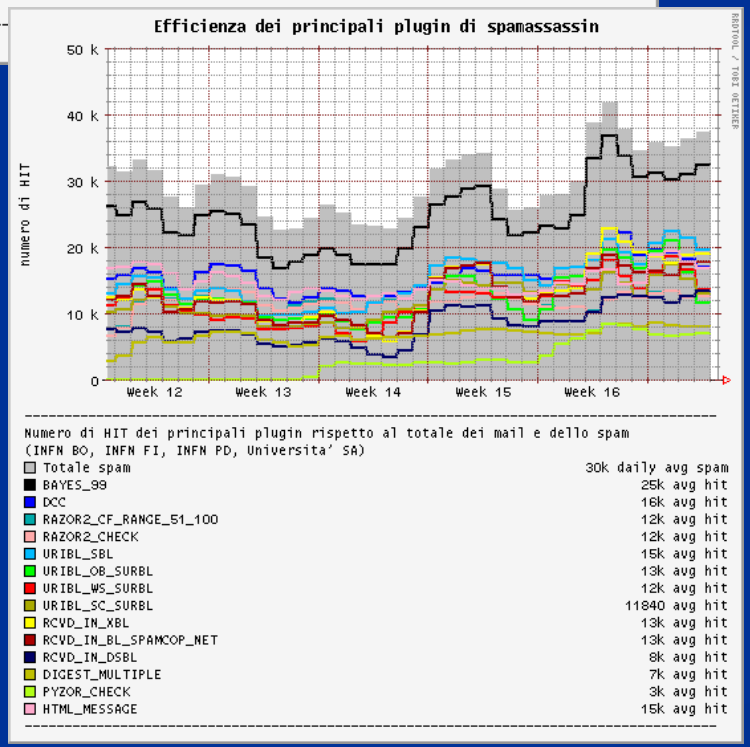
Attività anti-spam

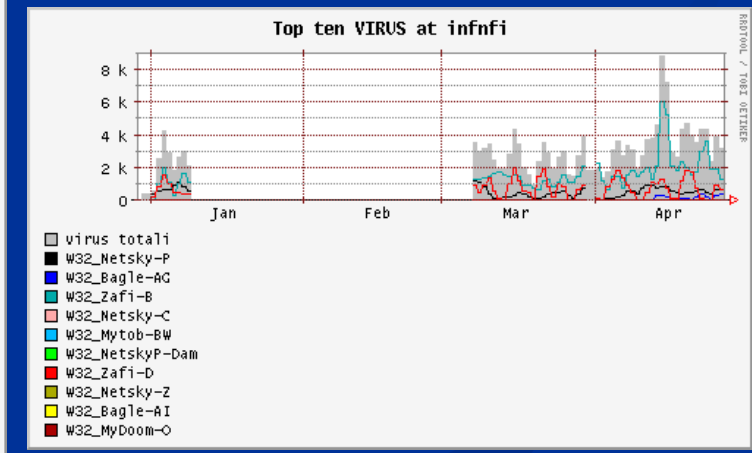
- Studio e miglioramento dell'efficienza di SpamAssassin (SA):
  - monitoraggio;
  - filtri bayesiani;
  - Real Time Block List (RBL);
  - sistemi "cooperativi".
- Sperimentazione di sistemi alternativi:
  - Bogofilter: http://bogofilter.sourceforge.net/
  - DSPAM: http://www.nuclearelephant.com/projects/dspam/

Monitoraggio









Filtri bayesiani

- I filtri “invecchiano” e vanno aggiornati.
- Aggiornamento manuale laborioso
  - aggiornamenti frequenti da campioni scelti dagli utenti, preferibilmente con db diversi per ogni utente.
- Aggiornamento automatico pericoloso
  - mail con l’unico scopo di “inquinare” il filtro.

Real Time Block List (RBL)

- Liste di nodi utilizzati per spedire spam
- Per ogni mail query DNS per verificare se il nodo mittente appare nella lista
- Verificare bene l'attendibilità del gestore.
- URI RBL controlla le URL nel testo del mail

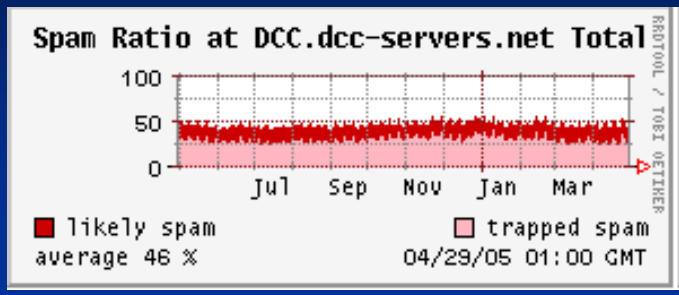
Sistemi “cooperativi”

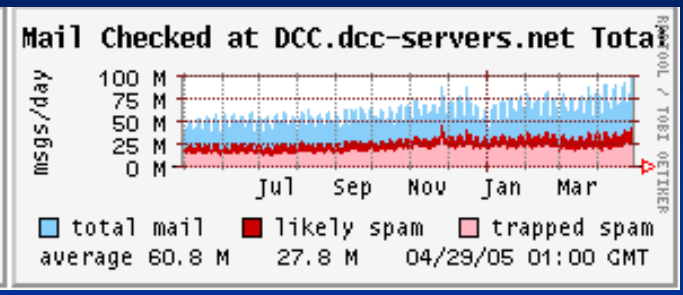
- Reti di server interrogati per ricavare la probabilità che il mail in esame sia spam
- Devono essere tenuti costantemente aggiornati
- **Razor**
  - gli utenti segnalano a mano i mail di tipo spam o ham
- **Pyzor**
  - tentativo di replicare Razor con software open source
- **DCC**
  - si basa sul fatto che i mail di spam vengono diffusi in grande numero

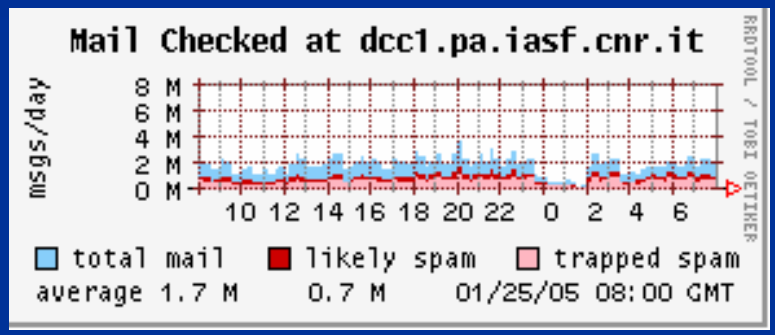
Rete GARR di server DCC

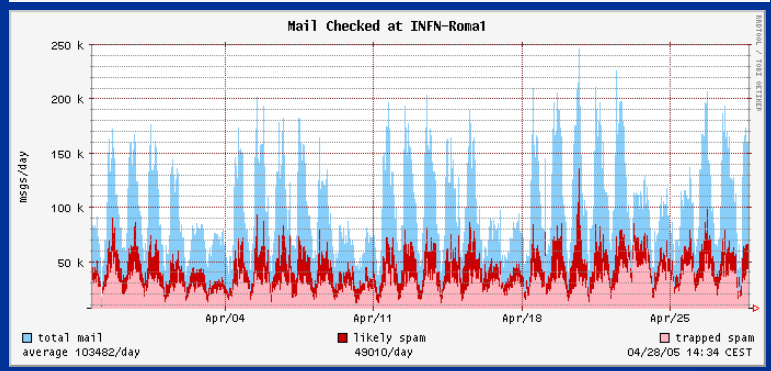
- Da Gennaio è in funzione una rete GARR di server DCC
  - INAF Palermo (G. Fazio)
  - INFN Torino (A. D'Ambrosio)
  - INFN Roma 1 (A. Forte e A. Spanu)
- Accesso privilegiato per utenti registrati (fare richiesta agli amministratori)

DCC: statistiche









- Server di IASF Palermo (in un giorno):
  - 800k richieste di checksum (70k da client autorizzati)
  - 1.2M report dai 25000 client
- Tempo di risposta medio 5ms

Best practice

- Aprire la porta 25 solo ai mail server autorizzati
- lasciare aperte le porte 587 e 468 per le connessioni ai server esterni
- permettere l'accesso ad utenti esterni autenticati (fondamentale per SPF)
- configurare l'antivirus per non mandare avvertimenti al mittente (sempre falsificato)
- "greet pause" su **sendmail** (≥ 8.13)
- non accettare i mail ritenuti spam?

Autenticazione del mittente

- Sender-ID
- Sender Policy Framework (SPF):
  - ogni dominio pubblica nel DNS i server **autorizzati** a spedire posta per quel dominio
  - il ricevente usa queste info per rifiutare mail da server non autorizzati (o per modificare il punteggio di sa)
  - L'utente esterno deve **sempre** usare il mail server di casa (autenticandosi)

Test di SPF

- Università di Salerno
  - un mese di durata
  - $650 \cdot 10^3$ mail
  - 32% da domini con informazioni SPF
    - 12% esterni
    - 20% interni

Sviluppi futuri

- Documento *best practice*
- Test di plugin SA “non ufficiali”
- Liste di plugin di SA consigliati
- Sperimentazione di SPF
- Completamento test Bogofilter e DSPAM
- Ampliamento rete DCC (e Pyzor?)