

WG sec-mail



O. Pinazza per il gruppo di lavoro

Il gruppo di lavoro

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



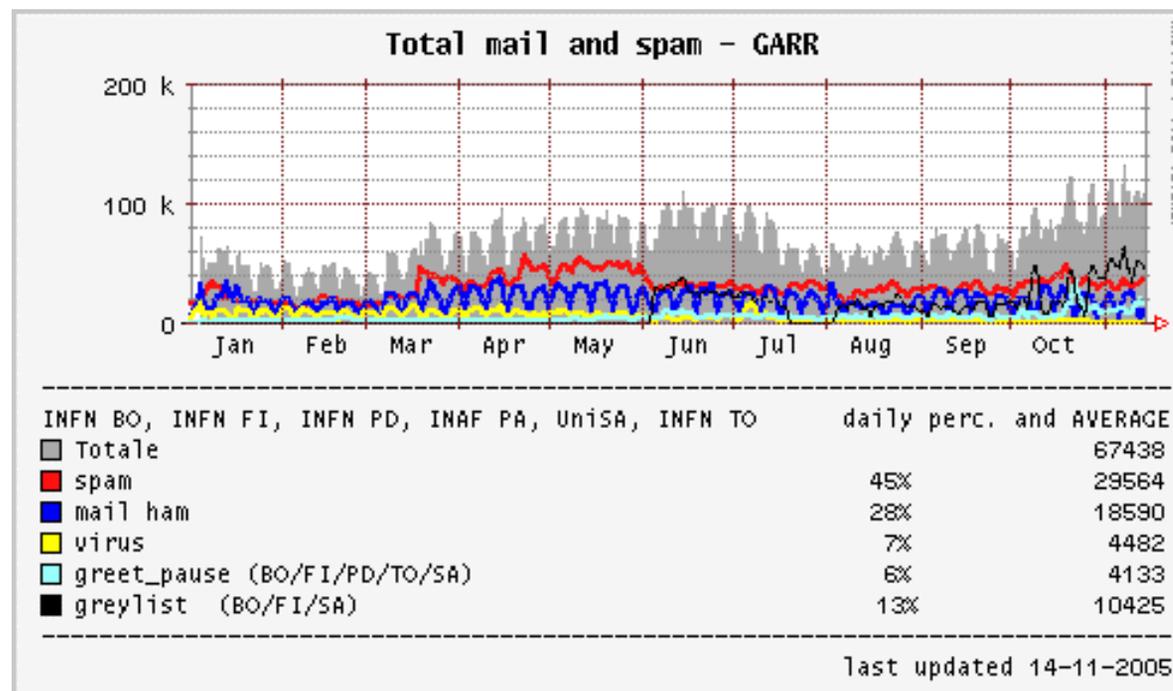
Risultati di due anni di lavoro

- Documenti
 - Best practice
 - Guide all'installazione e setup di base
 - Sito web e wiki
- Antispam
 - Spamassassin e plugin
 - Greylisting
 - DCC, Pyzor
 - Dspam
- Autenticazione del mittente
 - DomainKeys, SPF, SenderID



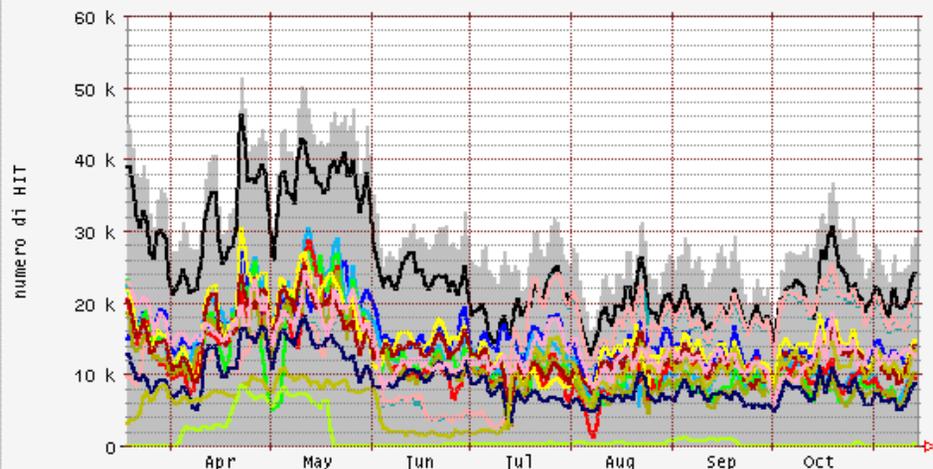
Spamassassin

- ❑ Spamassassin analizza il formato e il contenuto del messaggio e assegna un punteggio ad ogni caratteristica
- ❑ Se supera una soglia prestabilita, il messaggio è considerato spam



I plugin di spamassassin

Efficienza dei principali plugin di spamassassin

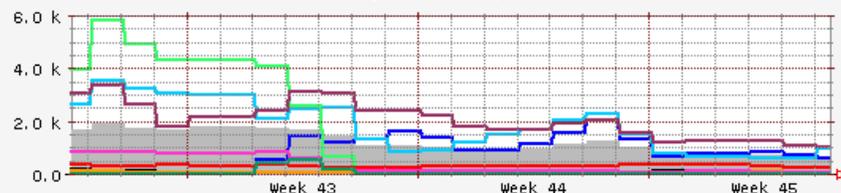


Numero di HIT dei principali plugin rispetto al totale dei mail e dello spam
(INFN BO, INFN FI, INFN PD, Universita' SA, INAF PA, INFN TO)

■ Totale spam	30172	daily avg spam
■ BAYES_99	24491	avg hit
■ DCC	15253	avg hit
■ RAZOR2_CF_RANGE_51_100	14650	avg hit
■ RAZOR2_CHECK	14722	avg hit
■ URIBL_SBL	13048	avg hit
■ URIBL_OB_SURBL	11592	avg hit
■ URIBL_WS_SURBL	11637	avg hit
■ URIBL_SC_SURBL	10987	avg hit
■ RCVD_IN_XBL	14521	avg hit
■ RCVD_IN_BL_SPAMCOP_NET	13370	avg hit
■ RCVD_IN_DSBL	8863	avg hit
■ DIGEST_MULTIPLE	8406	avg hit
■ PYZOR_CHECK	1187	avg hit
■ HTML_MESSAGE	13788	avg hit

last updated 14-11-2005

Totale hit di alcune famiglie di plugin nella sede infnfi



		eff	eff%	last hit	avg hit
■ Totale spam a infnfi				691	1208
■ plugin di tipo SARE	(395 test, avg score 1.599)	24	3.5	593	824
■ plugin di tipo RAZOR2	(3 test, avg score 0.783)	305	44.1	1251	1794
■ plugin di tipo URIBL	(7 test, avg score 2.402)	0	0.0	0	1460
■ plugin di tipo HTML	(144 test, avg score 0.689)	54	7.8	1128	2023
■ plugin di tipo DRUGS	(19 test, avg score 1.176)	0	0.0	16	71
■ plugin di tipo FORGED	(33 test, avg score 1.623)	7	1.0	71	80
■ plugin di tipo RCVD	(52 test, avg score 1.111)	3	0.4	92	335
■ plugin di tipo DCC	(1 test, avg score 3.000)	84	12.2	283	304
■ plugin di tipo PYZOR	(1 test, avg score 3.451)	0	0.0	0	45

eff, eff% e last hit sono riferite a 2005-11-13, avg hit e' calcolata sull'intero periodo



I sistemi antispam cooperativi

□ DCC

- ogni messaggio è caratterizzato da un checksum che viene calcolato e memorizzato dal server di posta che lo riceve
- L'insieme dei checksum di tutti i messaggi è scambiato con tutti gli altri server DCC tramite un meccanismo di flooding molto efficiente
- Se, dal confronto fra i checksum, molti server di posta risultano avere lo stesso messaggio, è probabile che il messaggio sia spam

□ RAZOR

- Sistema distribuito collaborativo a cui contribuiscono utenti registrati

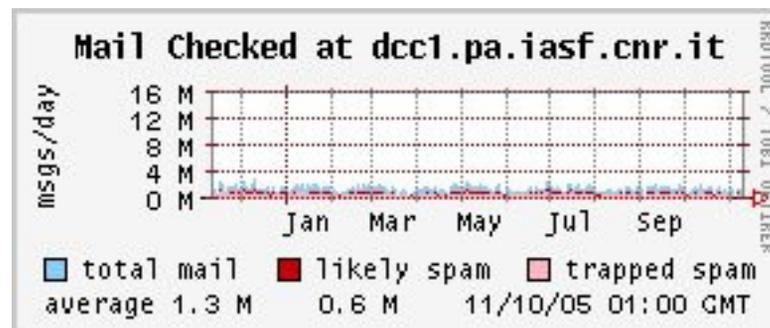
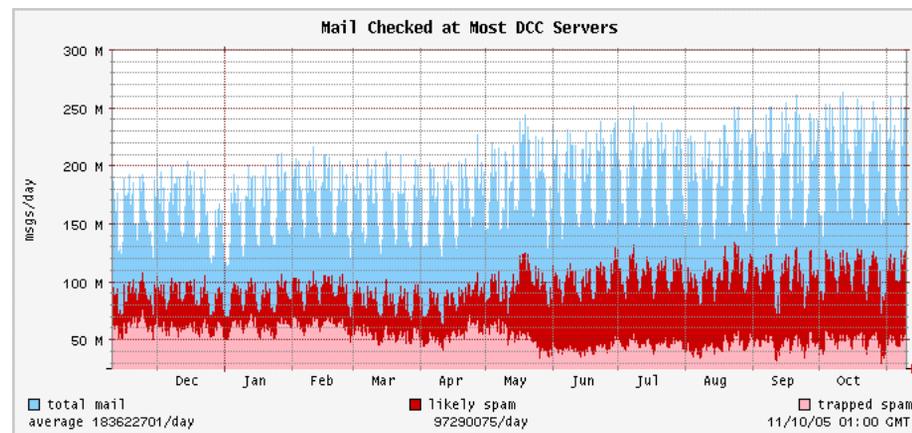
□ PYZOR

- Riscrittura opensource di Razor



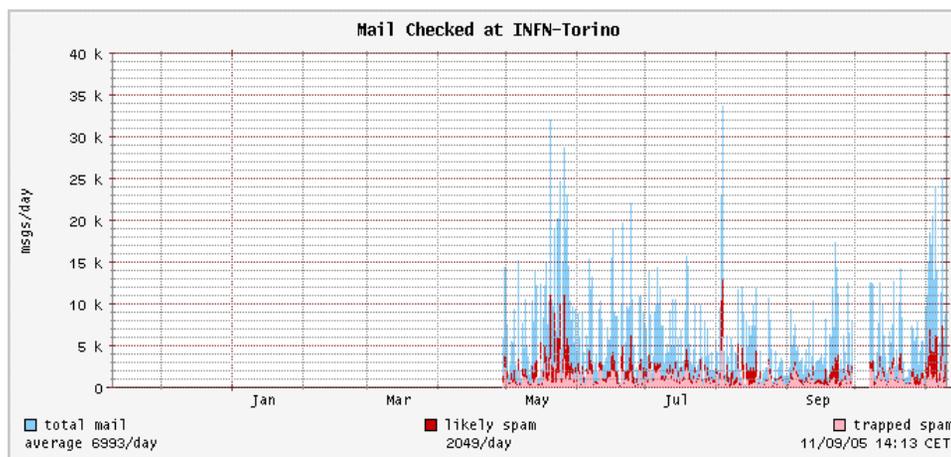
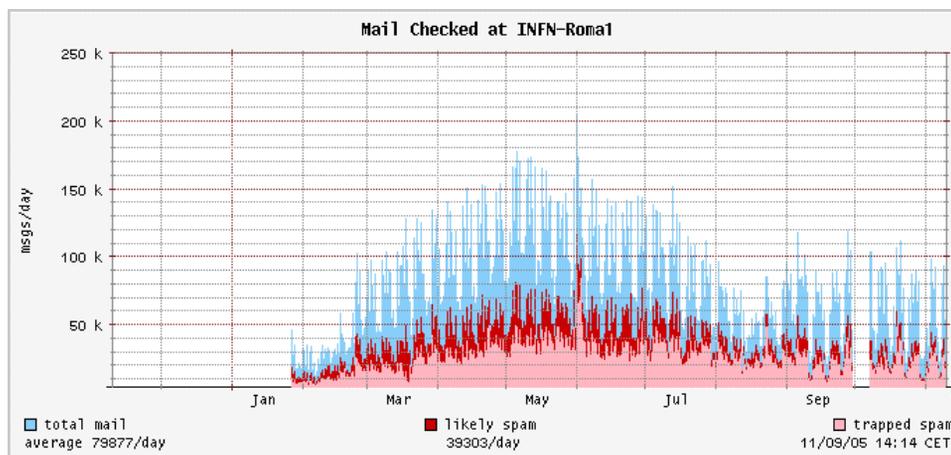
DCC (Distributed Checksum Clearinghouse)

- La rete di server DCC è costituita da decine di migliaia di client e più di 250 server
- Il primo server della rete GARR e primo server italiano è **dcc1.pa.iasf.cnr.it**



I server DCC di Roma1 e Torino

- DCC risponde sia a client registrati che anonimi, ma la priorità viene data ai client registrati
- Per utilizzare il servizio dei tre server GARR richiedere **id** e **pwd** agli amministratori dei server



Cosa fare dei messaggi SPAM?

- Li modifichiamo (es. Subject) per aiutare gli utenti a riconoscerli
 - Li spostiamo automaticamente in un folder
 - Li cancelliamo (su richiesta dell'utente)
 - Li rifiutiamo?
-
- L'importante è che l'utente sia informato e possa scegliere



Reject dei mail spam

- A Torino tramite AMaViS milter
- A Firenze tramite rjspam (milter) R.Veraldi@

- Come funzionano:
 - entrambi rifiutano il messaggio con un codice d'errore *permanente* (5xx) durante il dialogo SMTP, e il server mittente può decidere come procedere

 - Avvisare periodicamente gli utenti
 - Fare decidere agli utenti se vogliono o meno questo servizio
 - Mantenere un log del reject per eventuali controlli



Greylist

□ Il principio di funzionamento:

- Nuovo mail: si rimanda indietro con un codice d'errore *temporaneo*

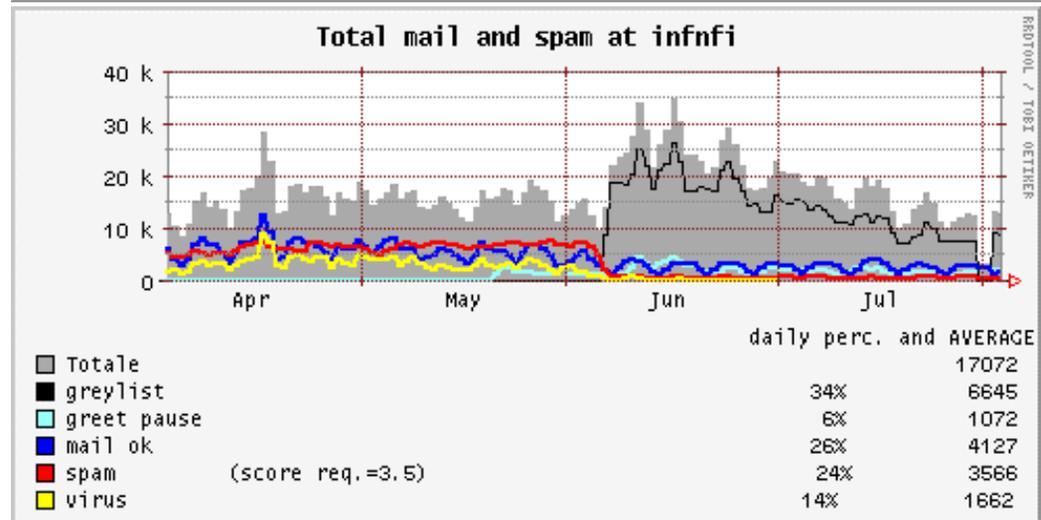
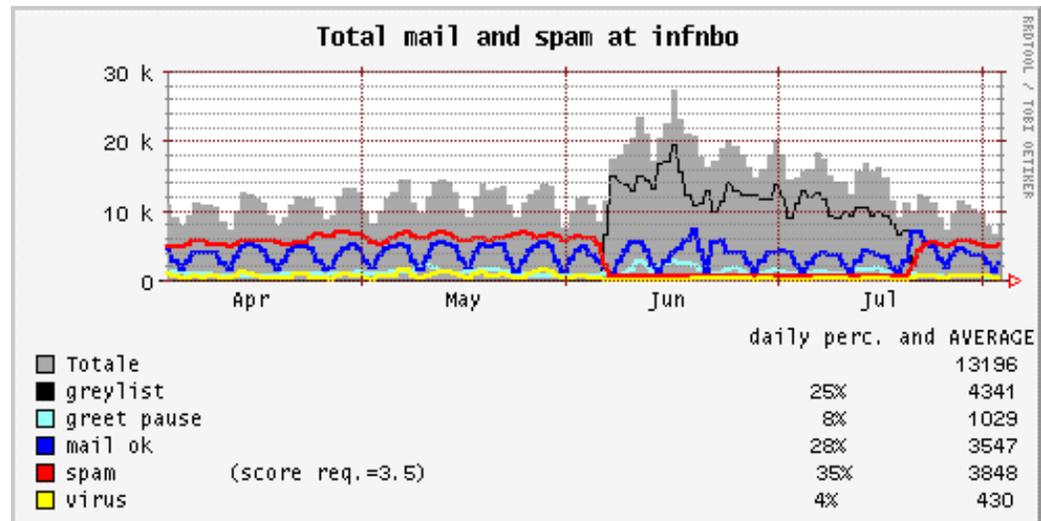
Nov 12 12:23:44 xmail sm-mta[94193]: jACBN9OW094193: Milter: to=<xxxxxxxx@yy.infn.it>, reject=451 4.7.1 Greylisting in action, please come back in 00:30:00

- Il server mittente riproverà dopo un tempo X
- Se l'intervallo di tempo richiesto è trascorso, il messaggio viene accettato e recapitato, e la terna [IP server mittente, mittente, destinatario] salvata in un DB
- Quando una terna si ripresenta, il messaggio è accettato senza ritardi
- I server spammer non implementano correttamente e completamente il protocollo SMTP e spesso non si fanno più vivi



1° effetto del greylisting (1/3)

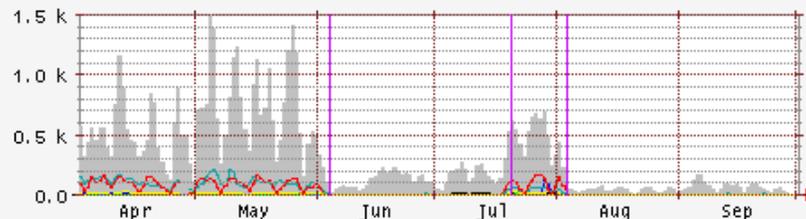
- I messaggi spam diminuiscono subito drasticamente
- Durante il primo periodo, il numero di messaggi in arrivo aumenta, ma si normalizza lentamente



2° effetto del greylisting (2/3)

- Sono diminuiti fortemente i messaggi con VIRUS!

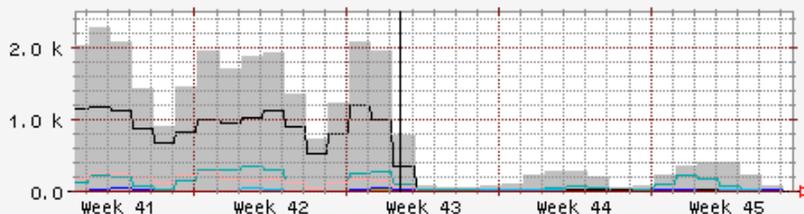
Top ten VIRUS at infnbo



- virus totali
- Worm. Mydoom. R
- Worm. Netsky. X
- Worm. Netsky. Q1
- Worm. Mytob. CR
- Worm. Mydoom. AZ
- Worm. Netsky. R
- Worm. Zafi. B
- Worm. Mytob. AC
- Worm. Netsky. C
- Worm. Mytob. MQ
- 4 giugno 2005 installazione greylis

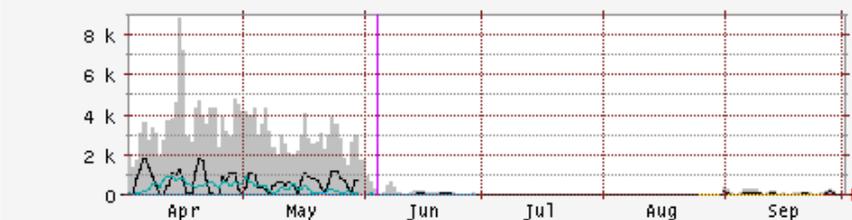
infnbo: no greylist dal 20/7 al 3/8

Top ten VIRUS at unisa



- virus totali
- W32_Netsky-P
- W32_Zafi-C
- W32_MyDoom-O
- W32_Netsky-C
- W32_Mytob-C
- W32_Netsky-B
- W32_Netsky-Q
- W32_Mytob-BE
- W32_MyDoom-N
- W32_Mytob-E
- 26/10/2005 installate greylis

Top ten VIRUS at infnfi



- virus totali
- W32_Zafi-D
- W32_Mytob-GH
- W32_Netsky-P
- W32_MyDoom-O
- W32_Bagle-AI
- Troj_Torpid-Gen
- W32_Bagle-P
- W32_Bagle-AN
- W32_Netsky-AD
- Troj_Sefex-A
- 4 giugno 2005 installazione greylis

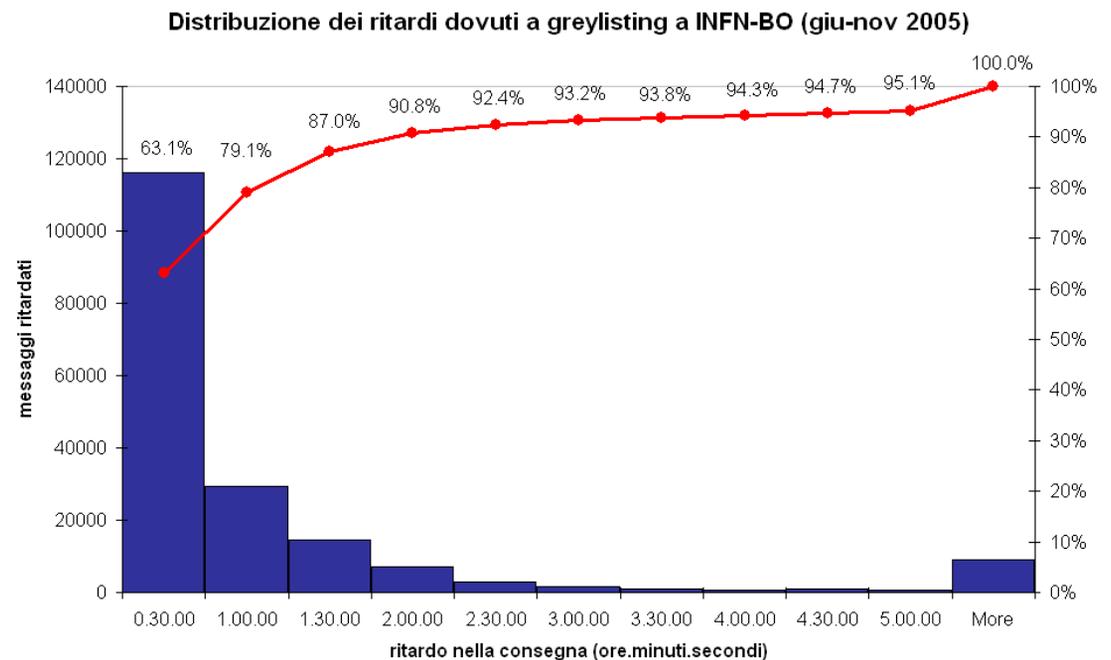
3° effetto del greylisting

□ Ritardo nella consegna del messaggio

- Nel primo periodo tutti i messaggi vengono ritardati e il ritardo non è prevedibile

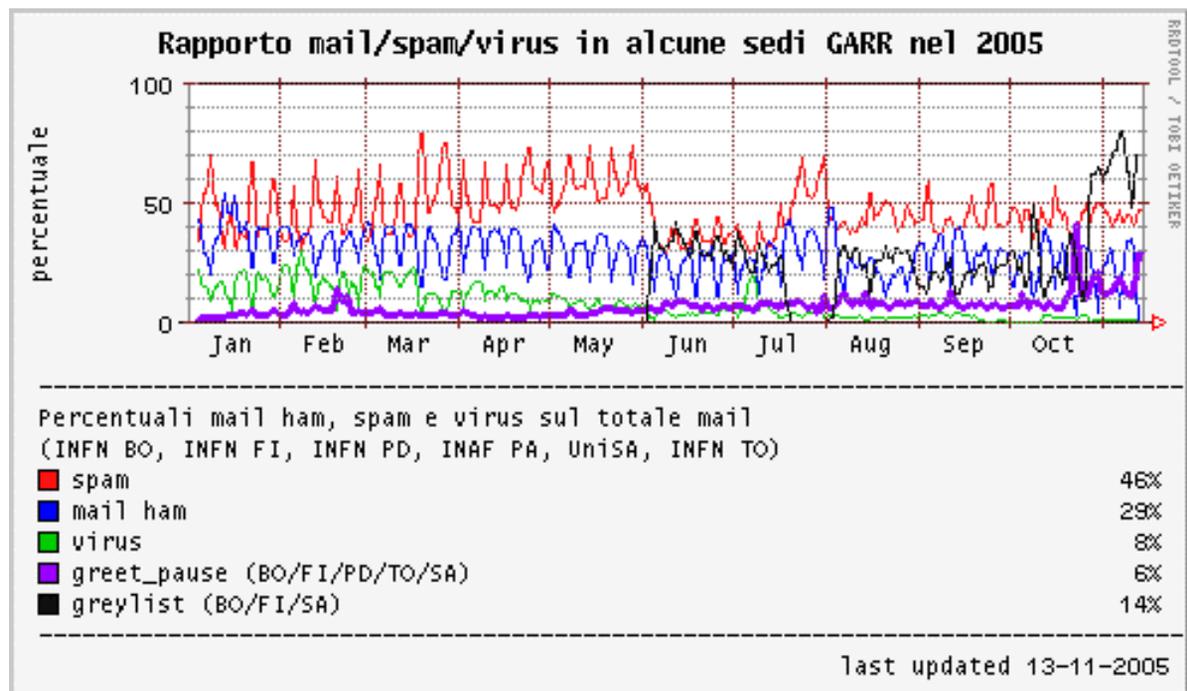
□ Altri problemi:

- alcuni MTA
- cluster di mailservers
- mail forwarders
- Mailing list



MTA: Sendmail, postfix, CGpro

- Controllo porte TCP 25 e 587
- Autenticazione mittenti (SMTP-AUTH, TLS, VPN)
- Greet_pause



Autenticazione dei mittenti

- Consentire il relay a client fuori dominio tramite
 - STARTTLS: tunnel TLS stabilito utilizzando certificati digitali
 - Autenticazione SMTP-AUTH
 - SMTP-AUTH funziona all'interno del tunnel TLS
 - L'autenticazione è basata su SASL e può utilizzare diversi meccanismi: PAM, kerberos, shadow, ldap...
 - VPN o webmail



Metodi di tipo “Sender authentication”

- Servono a dimostrare e proteggere l'identità del mittente, e combattere il problema del domain spoofing
- Autenticazione basata sull'IP (SPF/SenderID)
- Applicando una firma digitale ad una parte dell'header del messaggio (DomainKeys)



DomainKeys

- Meccanismo a chiave pubblica/privata
- Servono a convalidare il dominio del mittente

Mail header:

```
Received: from cernmxlb.cern.ch (cernmx05.cern.ch [137.138.166.161])
        by nasmal.bo.infn.it (8.13.3/8.13.3) with ESMTTP id jA7I4ChZ030619
        for <Ombretta.Pinazza@bo.infn.it>; Mon, 7 Nov 2005 19:04:17 +0100 (CET)
        (envelope-from xxxxxxxxxxxxxxx@cern.ch)
DomainKey-Signature: a=rsa-sha1; c=noaws; s=beta; d=cern.ch; q=dns;
        h=received:message-id:date:from:reply-to:to:subject:mime-version:content-
type:content-transfer-encoding;
        b=geDPwrSn/L2pBmyaeLBRRsmLVNk5XQYOFL5hcnfxdsuTJ8F/k3U. . . . rY7NvrNmiVLfgsr;
. . . .
From: Xxxxxxxxxxxxx <xxxxxxxxxxxx@cern.ch>
```

DNS:

```
beta._domainkey.cern.ch IN TXT "t=y; k=rsa; p=BHwwDQYJKoZIh....xMmcKwIDAQAB"
```



SPF e SenderID

- Il dominio identifica i propri mailserver pubblicando nel DNS un record SPF che descrive la propria policy
- Il mailserver che riceve i messaggi può richiedere e utilizzare questa informazione
- SPF = Sender Policy Framework (Classic SPF)
 - `bo.infn.it. IN TXT "v=spf1 mx ptr ~all"`
- SenderID (Microsoft)
 - `bo.infn.it. IN TXT "spf2.0/mfrom,pra ~all"`



Attività in corso

- Aggiornamento spamassassin
- Spf/SenderID
- DomainKeys
- installazione di un Pyzor server presso l'INAF-IASF di Palermo



Riferimenti

- Gruppo sec-mail:
 - <http://www.garr.it/WG/sec-mail/>
 - <http://secmail.unisa.it/doku.php>
 - <mailto:secmail-info@garr.it>

