# Amavis: un wrapper per antivirus su mailserver

Gennaro Tortone [tortone@na.infn.it]


Workshop CCR INFN – La Biodola – Maggio 2002

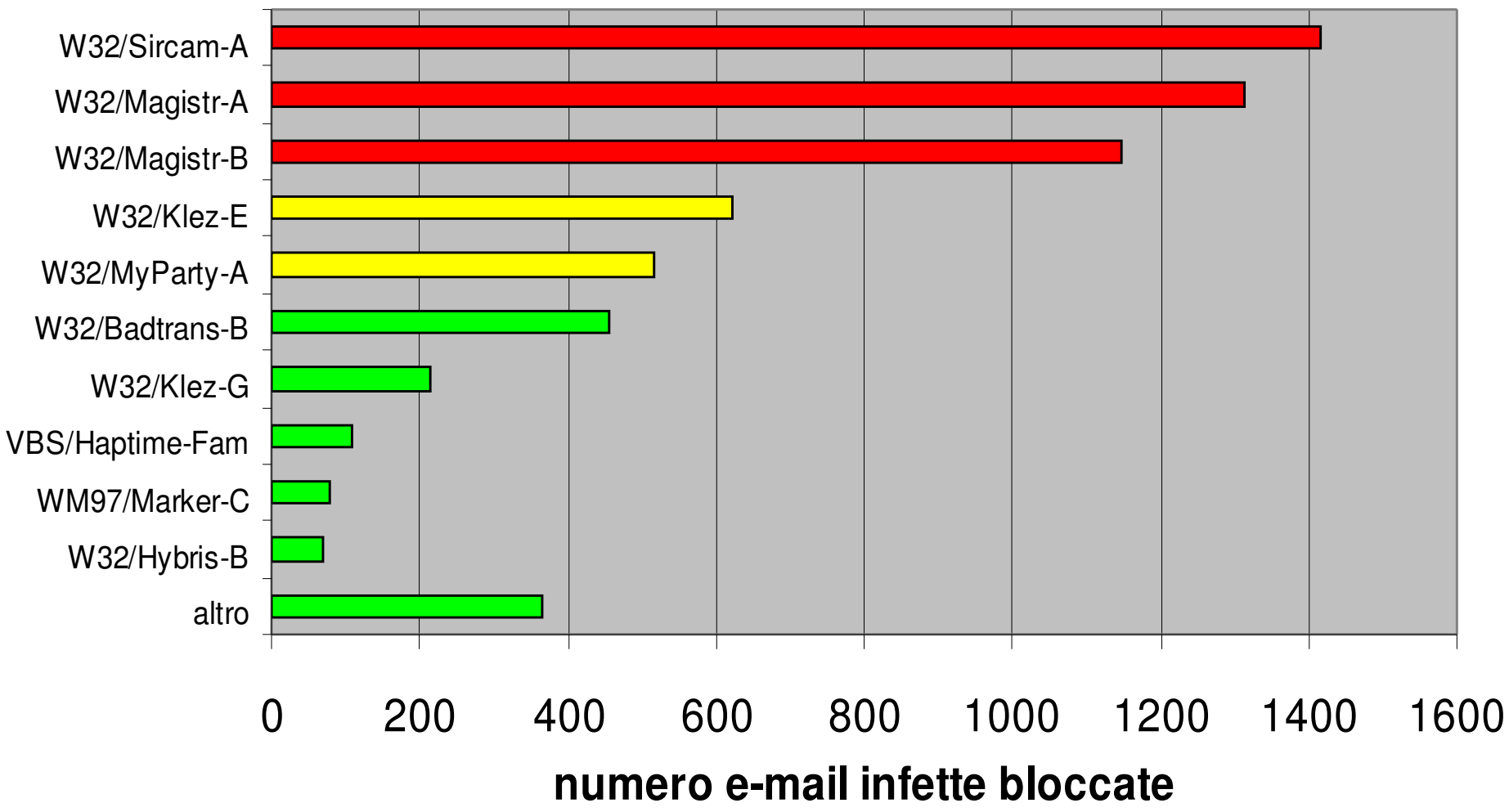
# Introduzione

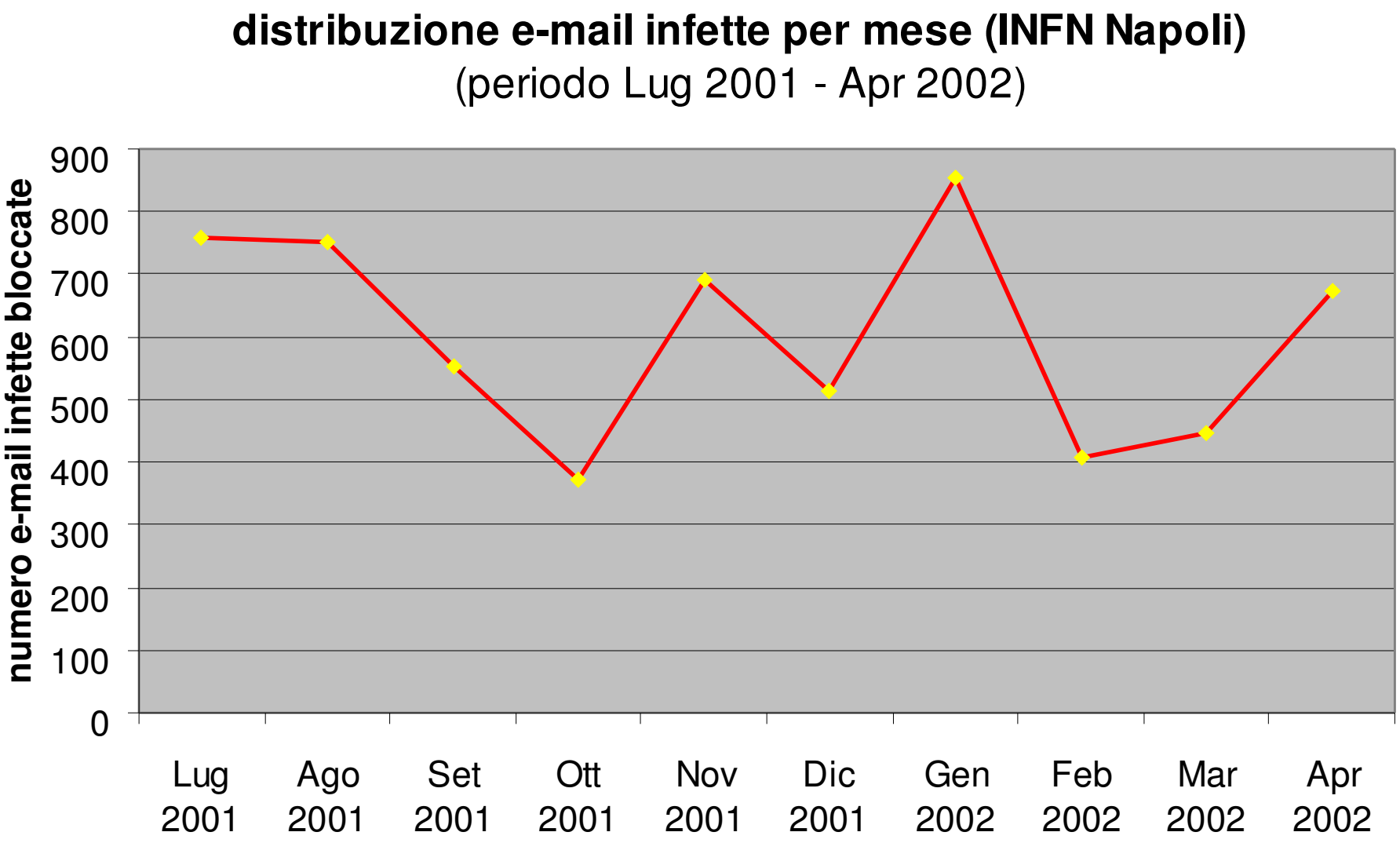
La posta elettronica e' diventata uno dei maggiori veicoli di diffusione dei virus;

Per far fronte a questo problema non basta l'installazione di antivirus su ogni singola workstation:

- molto spesso non vengono aggiornati (da parte dell'utente) i file di definizione dei virus;
- alcuni client di posta elettronica non sono supportati da determinati antivirus;

**Una buona soluzione al problema e' il filtraggio, a livello di mailserver, delle e-mail infette**


distribuzione e-mail infette
per tipologia di virus (INFN Napoli)
W32/Sircam-A
W32/Magistr-A
W32/Magistr-B
W32/Klez-E
W32/MyParty-A
W32/Badtrans-B
W32/Klez-G
VBS/Haptime-Fam
WM97/Marker-C
W32/Hybris-B
altro
0
200
400
600
800
1000
1200
1400
1600
numero e-mail infette bloccate


distribuzione e-mail infette per mese (INFN Napoli)
(periodo Lug 2001 - Apr 2002)
numero e-mail infette bloccate
900
800
700
600
500
400
300
200
100
0
Lug 2001
Ago 2001
Set 2001
Ott 2001
Nov 2001
Dic 2001
Gen 2002
Feb 2002
Mar 2002
Apr 2002

# Soluzione adottata

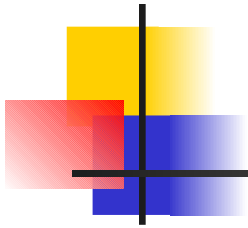
Amavis (A MAil VIrus Scanner)

- Amavis e' uno script Perl che interfaccia un MTA (Mail Transport Agent) con uno, o piu', virus scanner;
- Supporta Linux ed altre piattaforme UNIX (testato su Solaris, *BSD, AIX, HP-UX)


http://www.amavis.org

# Requisiti

1. Virus scanner
   - CyberSoft VFind
   - Dr Solomon's AntiVirus
   - F-Secure Inc. F-Secure AV
   - H+BEDV AntiVir/X
   - Kaspersky Anti-Virus
   - Network Associates Virus Scan
   - Sophos Sweep
   - Trend Micro FileScanner
   - CAI InoculateIT
   - GeCAD RAV AntiVirus 8
   - ESET Software NOD32
   - Command AntiVirus for Linux
   - VirusBuster
   - Sophie
   - Trophie
   - FRISK F-Prot
   - OpenAntiVirus ScannerDaemon
2. Decompressors
   - uudecode
   - compress
   - gunzip
   - unzip
   - unarj
   - unrar
   - xbin
   - LHArc
   - bunzip2
   - zoo
   - arc
   - freeze
   - tnef
3. Mime handlers
   - reformime
4. Mail Transport Agent
   - sendmail
   - qmail
   - postfix
   - exim
   - cyrus
5. File Type recognition
   - file

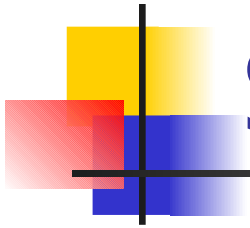


# Features

- supporto per i file attach compressi ricorsivamente;
- per ogni e-mail infetta e' possibile abilitare la notifica di:
    - postmaster
    - mittente
    - destinatario
- copia delle mail infette in “quarantine zone”;

Release history

- amavis 0.2.x: Bourne shell script;
- amavis-perl-1x: Perl script;
- amavisd: versione client server – lo script Amavis viene eseguito come daemon e comunica con il MTA mediante socket ed un programma client;



# Scenario di utilizzo

INFN Napoli

- n. 2 mail exchanger Linux (mx1.na.infn.it, mx2.na.infn.it);
- MTA Sendmail;
- amavis-perl-11
- Sophos Anti Virus per Linux (commerciale)

Punti di forza dell'architettura

- velocita' di scansione del software di antivirus;
- aggiornamento costante del file di definizione dei virus (ogni ora);
- scansione della posta in ingresso e in uscita;
- semplice integrazione di Amavis con Sendmail (aggiunta di poche righe al sendmail.cf);

# Conclusioni

L’utilizzo di Amavis rende indipendente la configurazione del mailserver rispetto al software di virus scanner utilizzato

e’ possibile cambiare antivirus senza modificare la configurazione del MTA