

red.es

XIV Grupo de Coordinación IRIS-CERT

Informe de Operación

Departamento RedIRIS

17 de Junio, 2004

Incidentes totales: 933 (↑ 80.46%)

- Infracción de copyright: 432 (144.48% ↑)

2002: 50

2003: 299 (498% ↑)

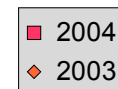
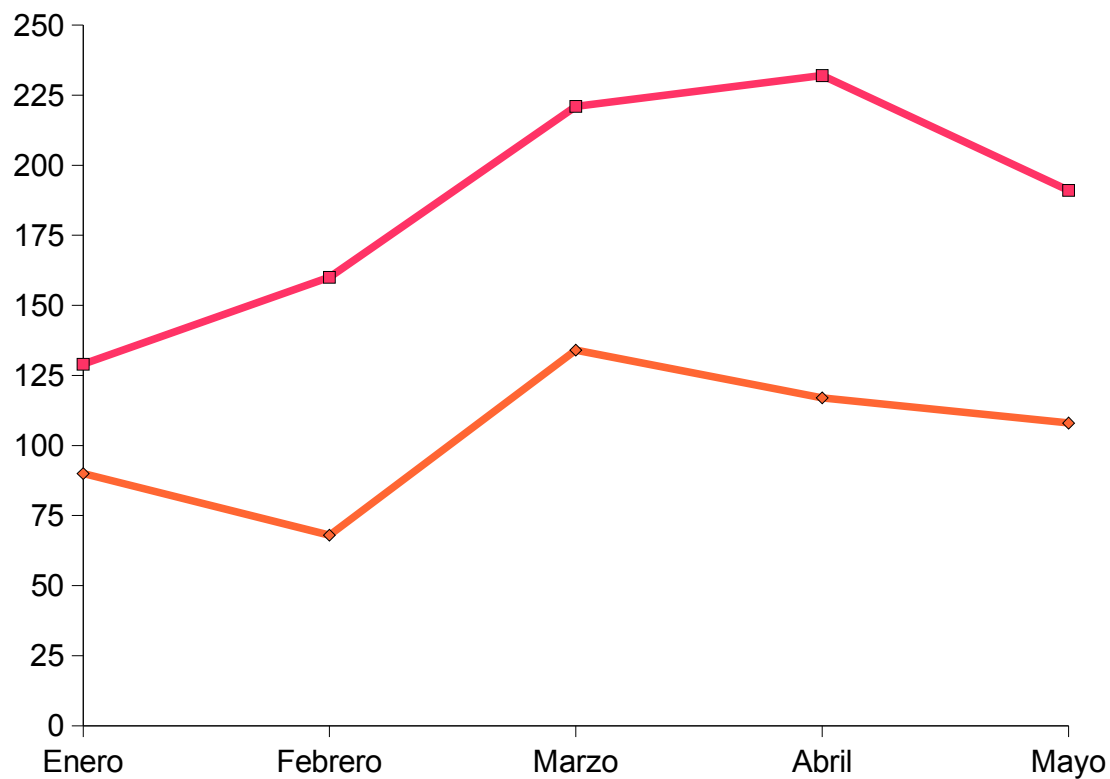
- Correos como Cc: 33

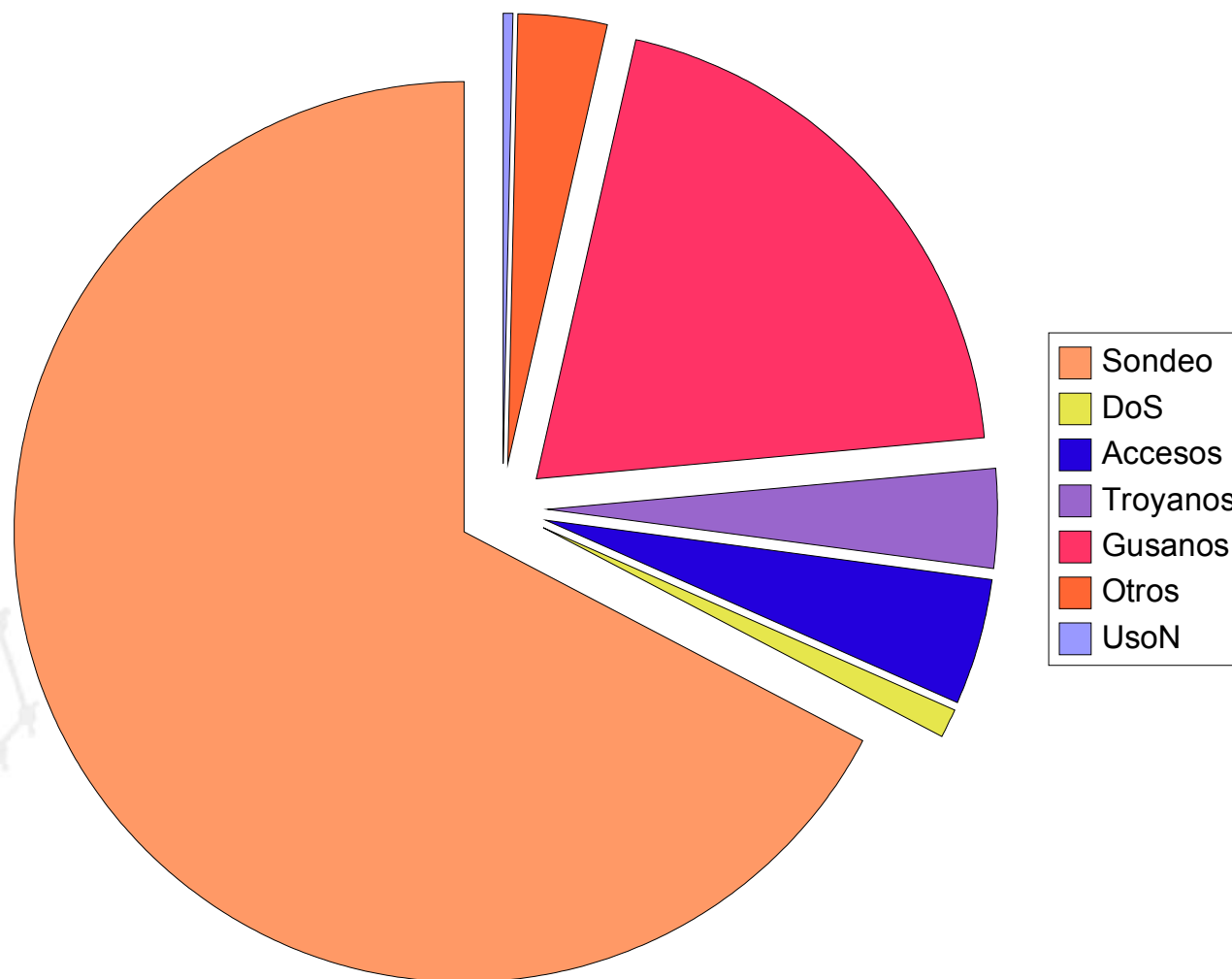
- *Helpdesk*: 27 (desde 19 Abril)

Total: 1425 (275.62% ↑)

Por origen de incidente:

- Comunidad RedIRIS: 921 (98.71%)
- Dominio .es (fuera de la comunidad): 2 (0.21%)
- Internacional: 10 (1.07%)





5554/tcp y 9898/tcp

- Dabber → <http://www.f-secure.com/v-descs/dabber.shtml>

443/tcp (SSL/TLS)

- *Microsoft Private Communication Technology (PCT)* → <http://www.kb.cert.org/vuls/id/586540>

5000/tcp

- *Microsoft Windows Universal Plug and Play service (UpnP)* → <http://www.microsoft.com/technet/security/bulletin/MS01-059.msp>

Phatbot (2745/tcp, 1025/tcp, 80/tcp, 5000/tcp, 6129/tcp, ...)

- http://www.f-secure.com/v-descs/agobot_fo.shtml

Sasser (445/tcp, 9996/tcp, 5554/tcp)

- <http://www.f-secure.com/v-descs/sasser.shtml>

Netbios, Dameware (6129/tcp), Radmin (4899/tcp), http,

A aplicar en todos los puntos de entrada a la red

- Tráfico no permitido

Sólo se permite tráfico hacia y desde los rangos asignados a cada institución → antispoofing

Rangos privados

- Limitación de tráfico

ICMP

Aplicaciones P2P

- ≤ 2 Mbps $\rightarrow$ 64 Kbits/s
- ≤ 100 Mbps $\rightarrow$ 128 Kbits/s
- ≤ 2.5 Gbps $\rightarrow$ 1 Mbit/s

- Filtros de aplicación

137-139/tcp-udp, 445/tcp-udp

El SPAM comercial “a secas” no es ya el principal problema

- SPAM causado por Virus/Gusanos
Que incluyen su propio motor SMTP
- Tráfico masivo producido por falsificación de cabeceras o direcciones “From:”

Posibles soluciones

- Filtro 25/tcp en salida
- Diversas iniciativas y enfoques (basadas en confianza y distribuidas)
Bonded sender, *Habeas*, *mail tld*.
SPF (*Sender Policy Framework*), AMTP (*Authenticated Mail Transfer Protocol*), RMX (*Reserve MX*), etc...
- Coordinación en la comunidad RedIRIS (IRIS-MAIL)
MAIL-ES (Foro de Coordinación de Administradores de Correo Electrónico)