XVI Grupo de Coordinación

IRIS-CERT

Informe de Operación

Departamento RedIRIS

Málaga - 26 de Mayo, 2005

Agenda

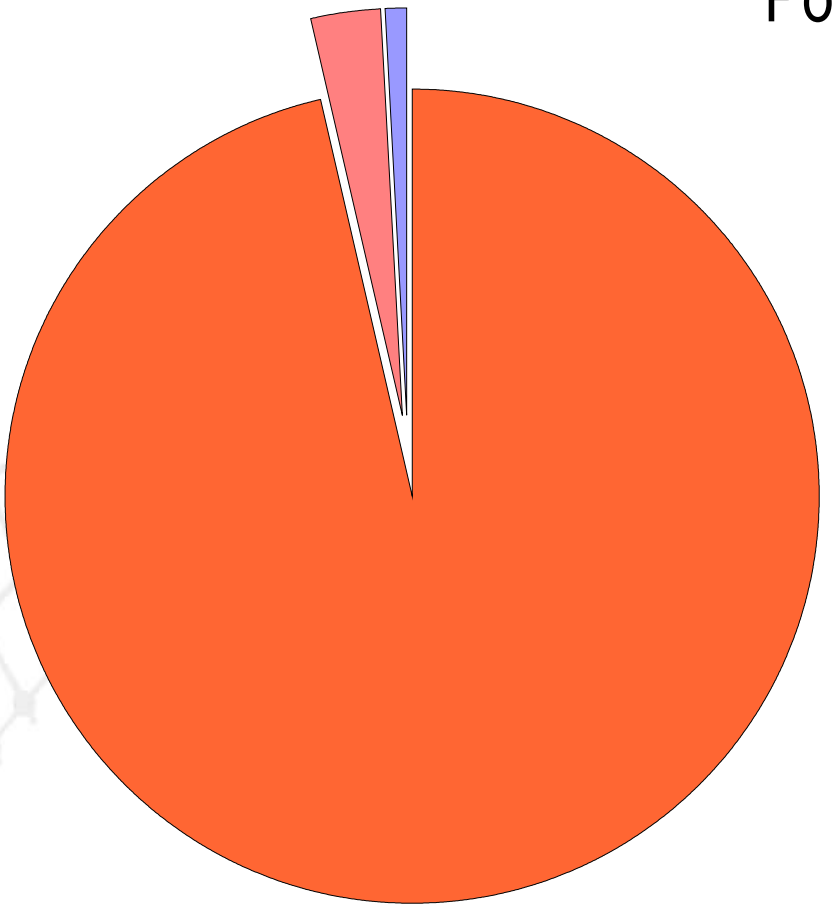
- Informe de operación IRIS-CERT
- Nuevas iniciativas
  - **ACRI** (Almacén Colaborativo de Reglas de Intrusión), Víctor Baharona, **UAM**
  - **EnREDA** (Entorno de Recogida de Evidencias Digitales y Análisis), Rafa Calzada, **UC3M**
  - **ANAMARIS** (ANálisis de Actividad MAliciosa y Respuesta a IncidenteS), Carles Fragoso, **CESCA**
- TrackUZ: Una propuesta para control de tráfico malicioso sobre Packeteer (c), Víctor Pérez Roche, **UNIZAR**
- Detección Ubicua de Ataques y Respuesta, Pedro García Teodoro, **UGR**

Informe de Incidentes
Enero-Mayo 2005

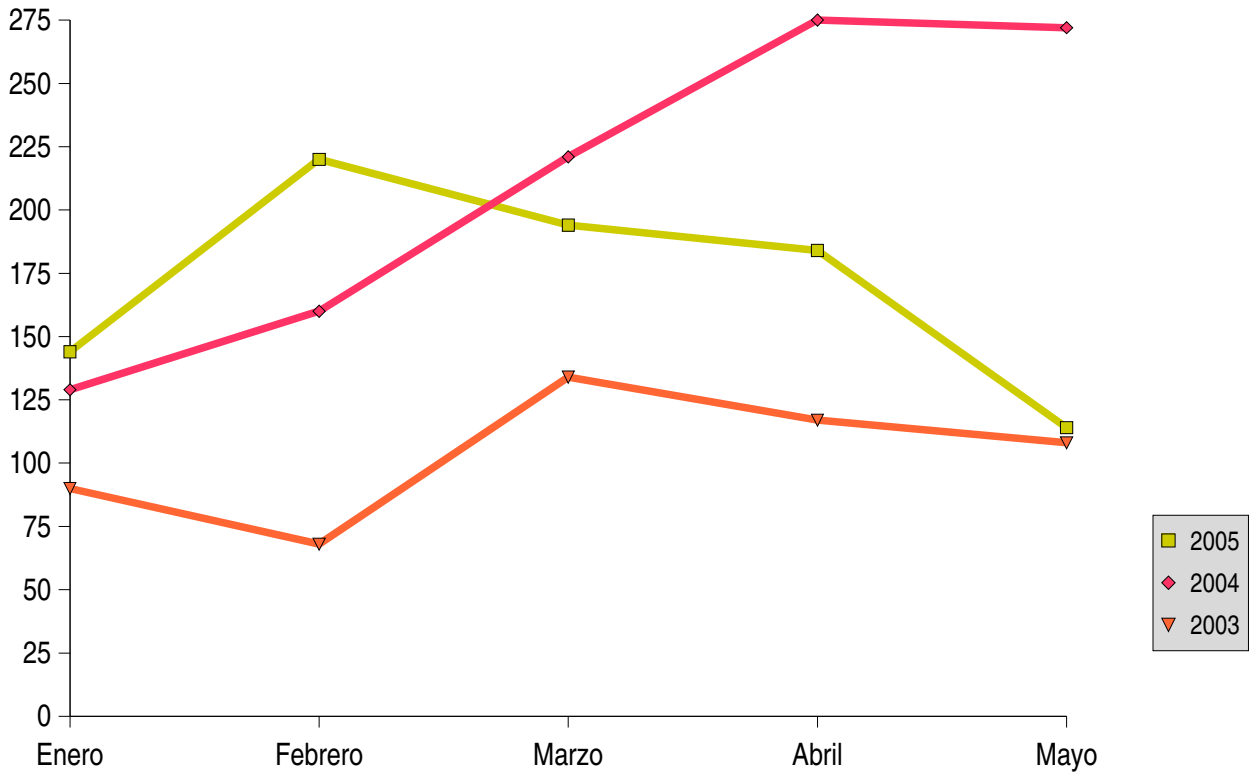
- Incidentes totales: 514 (↓ 44.90%)
  - Infracción de copyright: 312 (27.77% ↓)
    - 2002: 50
    - 2003: 299 (498% ↑)
    - 2004: 432 (44.48% ↑)
  - Correos como Cc: 11
  - *Helpdesk*: 10
  - Informativos: 9

Total: 856 (39.92% ↓)

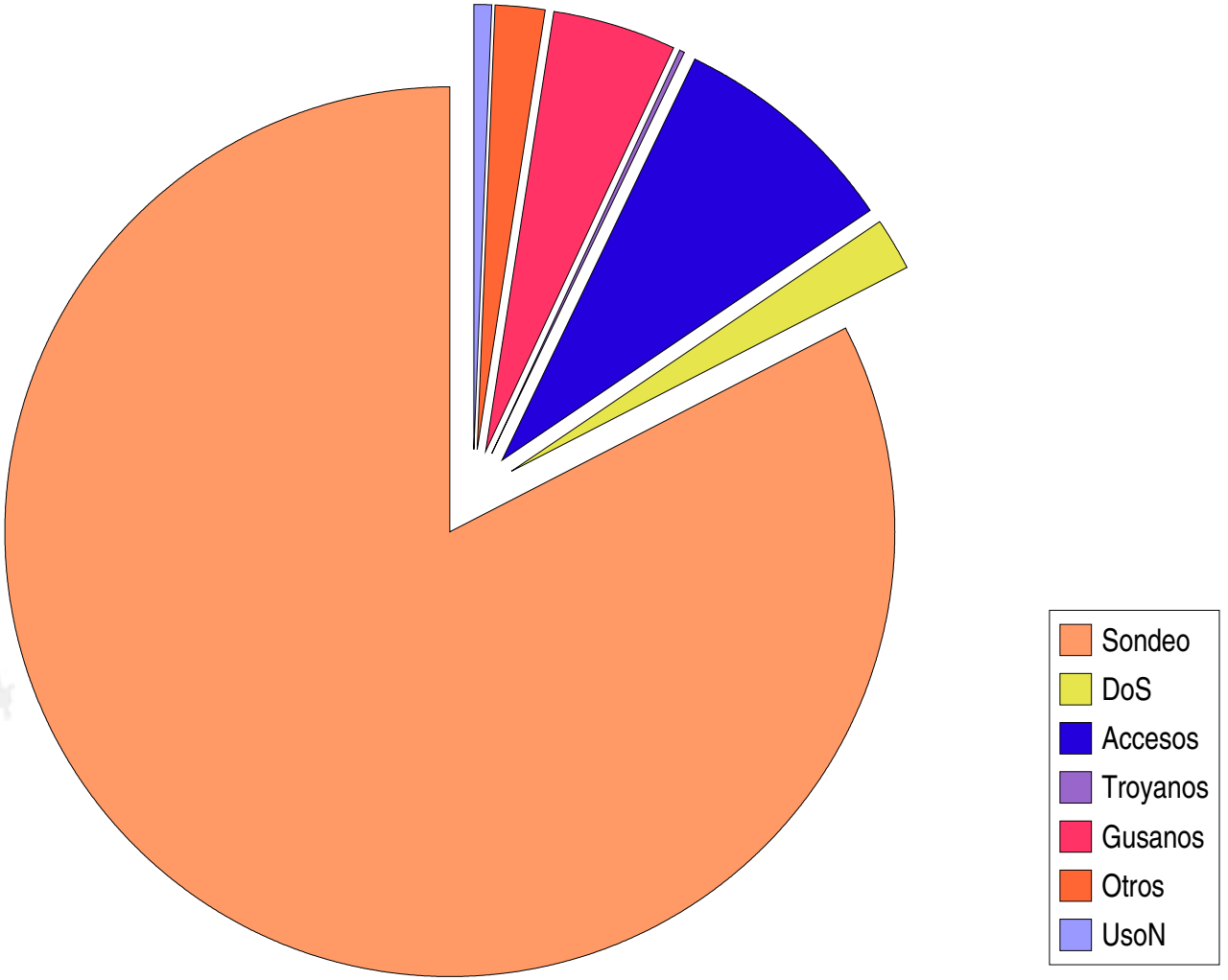
Por origen del inicidente



Informe de Incidentes
Enero-Mayo 2004



Informe de Incidentes
Enero-Mayo 2004



¿Qué hay ahora mismo activo?

- Ataques de fuerza bruta SSH (desde Julio 2004)
  - Cuentas con password por defecto
  - Utilización de exploit local
  - Instalación de diversos paquetes (bot IRC, herramientas de escaneo y DoS)
- Nueva versión del Beagle
  - http://alerta-antivirus.red.es/virus/detalle_virus.html?cod=4683
  - Muchas denuncias sobre máquinas empleadas como proxy http
    - http://www.rediris.es/cert/doc/gusanos-http.txt
- Veritas Backup Exec Agent (6101/tcp)
  - http://seer.support.veritas.com/docs/273419.htm
- Dameware (6129/tcp), WINS (42/tcp), Radmin (4899/tcp), httpd (80/tcp) etc...

Reto de análisis forense

- Menos participación de la esperada
- Máquina a analizar: Linux
- Ganadores
  - Victor Baharona (UAM), José Ignacio Parra y Quique López
  - Juan Martín Galeote - UGR
- Intención de cambiar el formato y repetir las ediciones (en colaboración con la Universidad de Méjico)

Geant2/JRA2 (Seguridad)

- Conjunto de utilidades para análisis de flujos
  - NFSen: interface gráfico para nfdump (para recolectar y procesar datos netflow)
    - http://nfsen.sourceforge.net/
    - http://sourceforge.net/projects/nfdump/
  - NERD *(Network Emergency Responder & Detector)*
    - http://beveiliging.surfnet.nl/info/innovatie/nerd.jsp

Eventos 2005

- Nuevas ediciones de cursos TRANSITS (finales 2005/mediados 2006)
  - http://www.ist-transits.org/
  - http://www.first.org/
- Cursos SANS Madrid (Junio 2005)
  - http://www.sans.org/madrid2005/
- Cursos SANS Barcelona (Octubre 2005)
  - http://www.sans.org/barcelona2005/
- Mesa redonda análisis forense (Septiembre 2005)
  - Aniversario 10 años IRIS-CERT

Nueva iniciativa

- Red de recolectores de Malware
  - Basada en mwcollect
    - http://www.mwcollect.org
  - + script de informe diario
- Recolección de gusanos y bots
- Cada participante instalaría los sensores en los equipos que considere
- Permitiría la detección del tipo de binario empleado en muchos ataques
- Permitiría detectar máquinas internas infectadas