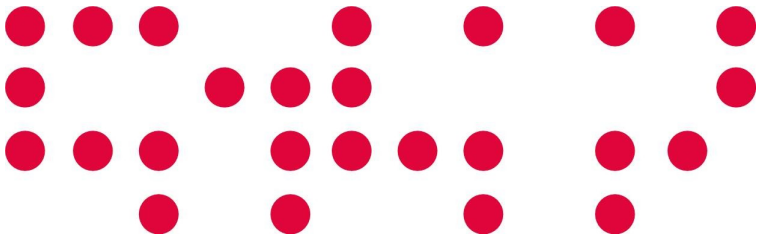
Grupo de Trabajo IRIS-CERT

XXIII Grupos de Trabajo de RedIRIS

Madrid, 26 Junio 2007

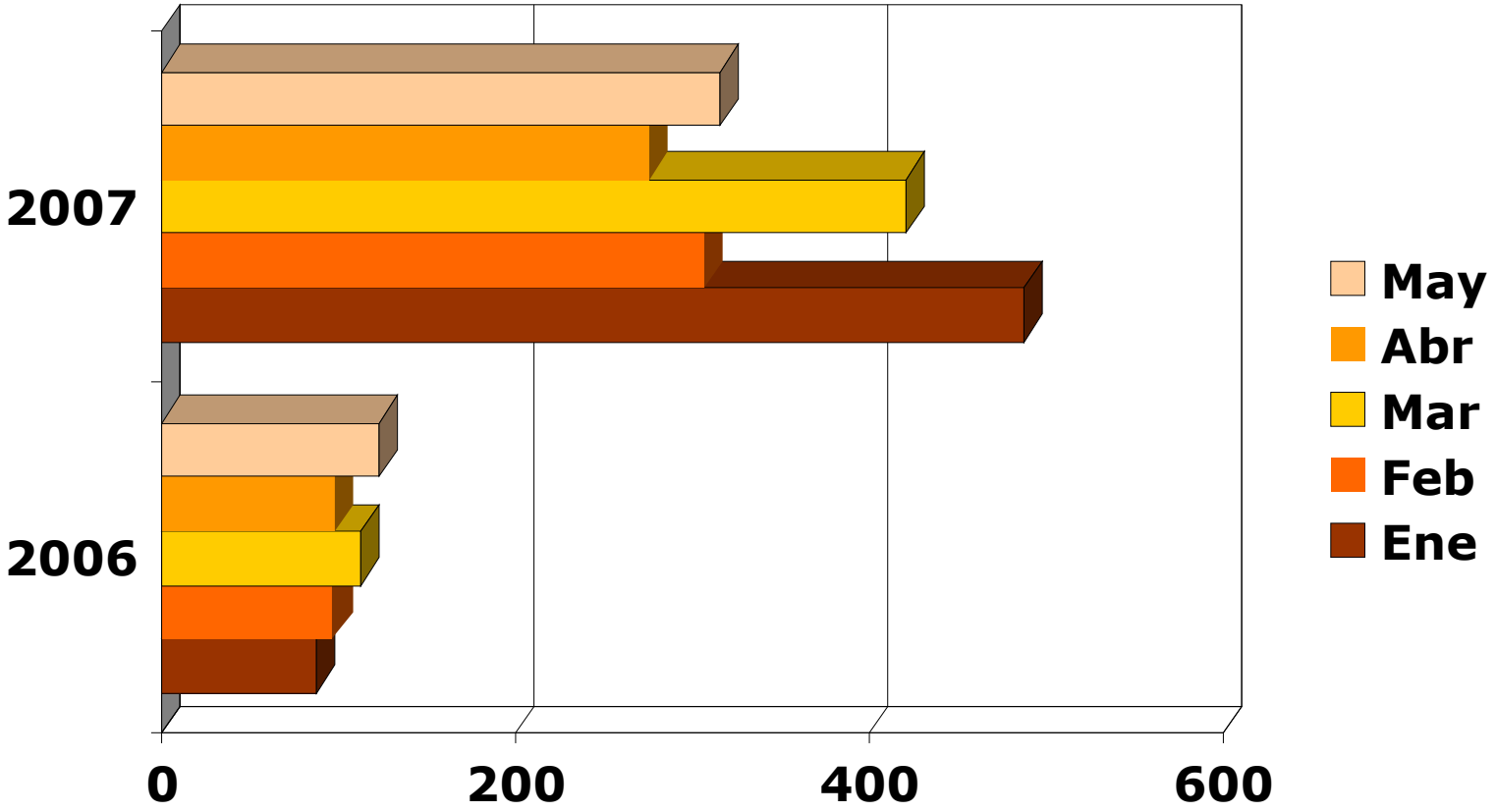
Agenda

- Nuevos CERTs en el panorama nacional
  - CCN-CERT, *Antonio Sánchez*
  - INTECO-CERT, *Francisco A. Lago*
- ArCERT (CERT Gubernamental Argentino), *Gastón A. Franco*
- Informe de operación IRIS-CERT, *Chelo Malagón*
- Actualidad forense, *Francisco Monserrat*
- Actualidad iniciativas en la comunidad RedIRIS
  - DesconII (Desconexión temprana de máquinas comprometidas), *Rafael Calzada - UC3M*
  - Cancerbero (El perro guardián de los puertos), *Victor Barahona - UAM*



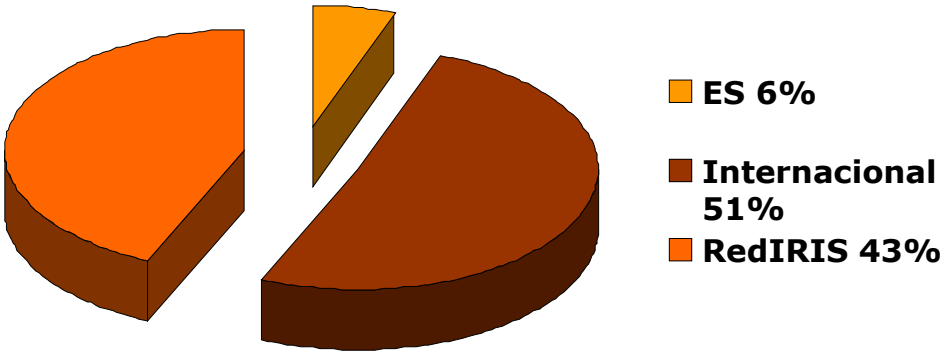
Informe IRIS-CERT (I)

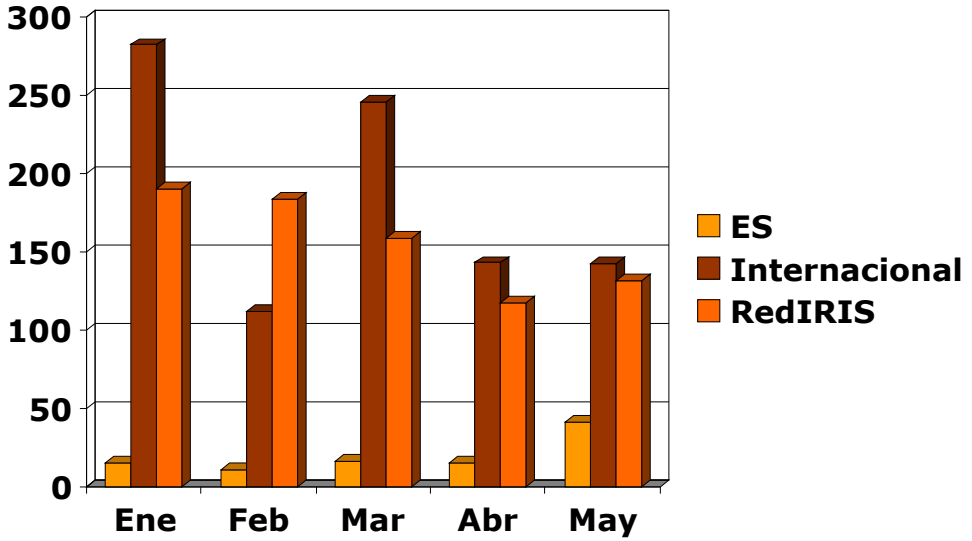
- 248%↑ con respecto al mismo periodo de 2006
  - 518 (2006) ➔ 1805 (2007)
    - 20 corresponden a *HelpDesk*
  - 75% (1357) de incidentes recibidos desde sistemas automáticos
    - 35% (473) en máquinas en la comunidad RedIRIS



Informe IRIS-CERT (II)

- 717 Incidentes sin respuesta
  - 492 de ellos corresponden a la comunidad RedIRIS





Informe IRIS-CERT (III)

- Y la cosa no cambia ….
  - Intentos de acceso no autorizados
    - Aprovechando vulnerabilidades conocidas o contraseñas débiles (ssh)
      - Educar a los usuarios en el uso de passwords fuertes
      - Mantener sistemas/aplicaciones actualizadas
  - Ataques a sistemas Web vulnerables
    - Vulnerabilidades conocidas en PHP
    - Inyección de código
  - Phishing y troyanos bancarios
    - Sobre todo en ISPs
  - Ataques dirigidos a aplicaciones más que a S.O

En muchos casos se trata de máquinas zombies, pero … no somos adivinos ;-)

Informe 2006

http://www.rediris.es/cert/doc/informes/2006/

TERENA TF-CSIRT (I)

- Continua el trabajo en las distintas actividades
  - CSIRTS&Grids, RTIR WG, colaboración con terceras partes (ENISA, FIRST, E-COAT, RIPE, JRA2, …)

    http://www.terena.org/activities/tf-csirt/

- TRANSITS (5-6 Julio, Sofía - Bulgaria)
  - Esponsorizado por ENISA
  - TERENA seguirá organizando 3 cursos al año en Europa mientras haya interés
  - Curso *"Técnicas y métodos de gestión y respuesta a incidentes de seguridad en red"* (9-13 Julio, La Bañeza - León) - INTECO
    - IRIS-CERT impartirá varias sesiones basadas en el material TRANSITS
      - http://www.inteco.es/frontinteco/es/frontIntecoAction.do?action=viewCategory&id=6771&publicationID=48073

- RTIR WG
  - Finales de Octubre 2007: Finalización 3º MileStone
    - Versión 2.2 estable y disponible para su uso
    - RT 3.7.4/RTIR 2.1.5/RTFM 2.2
      - ftp://ftp.rediris.es/rediris/cert/rtir/2ndMileStone/
  - Algunas funcionalidades de RTIR integradas en RT
    - GnuPG
    - Herramienta de eliminación de tickets
  - Documento de actualización
    - ftp://ftp.rediris.es/rediris/cert/rtir/migration.pdf
    - Incluso para RT

- Parte del OSCT (*Operational Security Coordination Team*) de EGEE-II (*Enablig Grids for E-ScienE*)
  - CSIRT del EGEE-II
  - CSIRT para SWE
  - Realizando labores de puesta en marcha del CSIRT
    - Implantación del RTIR
    - Definición de canales de transmisión de información
      - A nivel de incidentes
        - definición del flujo de atención de incidentes
      - Para los canales de coordinación
        - jabber, chat room
  - Dando formación de seguridad para GRID sites

- Y3 (hasta Enero 2008)
  - Poner las bases para hacer de Geant2 una comunidad tan segura como se necesita durante el Y4
    - Desarrollo de un conjunto integrado de herramientas ("Toolset") madura para su utilización por parte de los CERTs de GEANT2
      - FlowMoon Probe (http://www.flowmon.org/)
      - Nfsen/Nfdump
      - Detección avanzada de anomalías (Holt Winter extensión, DDoSVaX)
        - NetReflex (Anukools detection algorithm - http://cs-people.bu.edu/anukool/pubs.html)
      - Proceso de desarrollo abierto y coordinado con miembros del JRA2 para el nfsen
        - Criterios comunes para la incorporación de extensiones
    - Tener una idea clara de las expectativas de seguridad para GEANT2
      - Nuevo deliverable ➔ *GN2 Security Service Specification* (Definición de estándares de seguridad)
      - Actualmente trabajando en el *GN2 Service Roadmap*
        - Guía para el servicio de mentoring, identificación de NRENS a proporcionar el servicio (7), reparto de tareas - SWITCH, RedIRIS, GARR
        - Posible módulo de formación sobre Toolset a celebrar en Dante
    - Información pública sobre las actividades de seguridad en GN2

      http://www.geant2.net/cert/

- Y4+6 meses (Feb 2008)
  - Ayudar a que las NRENs socias de GEANT2 a que alcancen los estándares de seguridad estipulados
    - Formación
    - Mentoring Services (*CERT Web-of-Trust*)
  - Conseguir una "ToolSet" mejorada
    - Detección de anomalías
    - Inclusión de otras herramientas a medida que sean maduras
  - Promover la colaboración en materia de seguridad
    - No se han identificado todavía áreas de colaboración

- Nfsen/nfdump en producción desde Mayo 2006
  - Algunos routers del backbone sin monitorizar
  - 350 GB de flujos (28 días)
  - Uso de DesconII (UC3M) como agregador de alarmas
    - Evaluación otros agregadores para correlar información de todos nuestros sistemas de detección (prelude ¿?)
- En la actualidad trabajando en
  - Evaluación de la última snapshot de nfsen/nfdump
    - nfdump-snapshot-20070312/nfsen-snapshot-20070312
  - Adaptación de *Holt-winter Aberrant Behavior extension*
    - http://bakacsin.ki.iif.hu/~kissg/project/nfsen-hw/
  - Evaluación extensión nfsen-overflow
    - http://sourceforge.net/projects/nfsen-overflow/
  - Nuevos plugins de detección

http://sourceforge.net/projects/{nfdump/nfsen}

- 19th Annual FIRST Conference - 17-22 Junio (Sevilla)
  - *Network Monitoring Interest Group* (NM-SIG)
    - Compartir información/proyectos
    - Creación de una darknet entre los miembros del FIRST

      http://first.org/global/sigs/monitoring/
  - FIRST SC
    - Tenemos a uno de los nuestros entre ellos ;-)

  http://first.org/conference/2007/

- Reunión de coordinación de CERTs con competencias nacionales - 23-25 Junio (Madrid)
  - Organizada por el CERT/CC
  - Hemos hablado de botnets, honeynets, phishing, malware, herramientas, coordinación … ➔ Grupos de interés para trabajar en distintas áreas

- IV reunión celebrada en Madrid (28 Feb-1 Mar)
  - Whitelisting Española (ESWL/MTAWL)
    - http://www.rediris.es/abuses/eswl/
  - Proyecto SpamTraps
  - Apoyo y difusión de tecnologías emergentes
    - Nota de prensa promoviendo el uso de SPF
    - Compromiso para la implantación SPF entre los miembros
    - Estudios sobre adopción de otras soluciones (p.e DKIM)
  - Adopción BCPs entre ISPs
  - Revisión marco de adhesión al Foro Abuses
  - Cualificación de incidentes graves para actuaciones globales

http://www.rediris.es/abuses/

THE END .....

¿Alguna cosita más?

Edificio Bronce
Plaza Manuel Gómez Moreno s/n
28020 Madrid. España

Tel.: 91 212 76 20 / 25
Fax: 91 212 76 35
www.red.es