Jornadas Técnicas

RedIRIS. Noviembre 2003

XIII Grupo de Coordinación IRIS-CERT

Informe de Operación

IRIS-CERT
cert@rediris.es

Agenda

- Informe de operación de IRIS-CERT
- Tecnologías de flujos en Red (Netflow) para la detección de intrusiones y análisis forense.
  - *Francisco Monserrat (RedIRIS)*
- Aplicación de Control de Puertos Lógicos.
  - *M. Titos Ramis, M. Oliva Suárez (UIB).*

Café (11:30-12:00)

- Hackers en los Centros: Colaboración entre la Universidad de Vigo y La Guardia Civil frente al delito informático
  - *Jose Luis Rivas López (UVIGO)*
  - *Gonzalo Sotelo Seguín (Unidad Orgánica de Policía Judicial. Comandancia de la Guardia Civil de Pontevedra)*
- Securización de servidores Windows 2000
  - *Rafael Calzada (UC3M)*
- Detección de Intrusos: Estrategias y Herramientas
  - *Jess García (LAEFF)*

Informe de Operación de IRIS-CERT

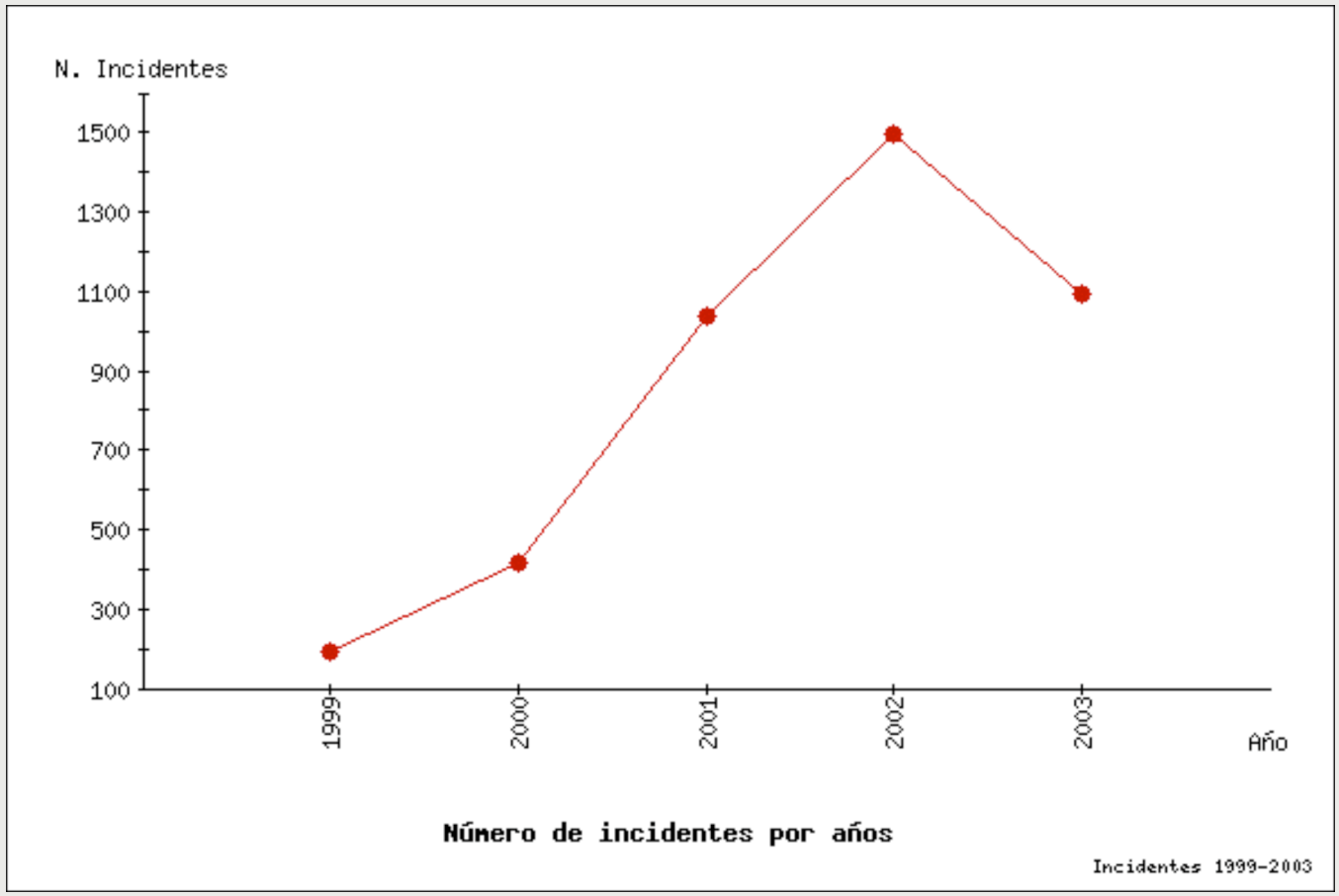
Agenda

- Informe de operación
- Foros nacionales
  - ESPX-CERT
- Foros Internacionales
  - FIRST
  - TERENA TF-CSIRT
- Otras actividades
  - Proyecto eCSIRT.net
  - Objeto IRT-IRIS-CERT
  - Reto análisis forense
  - Próximos eventos

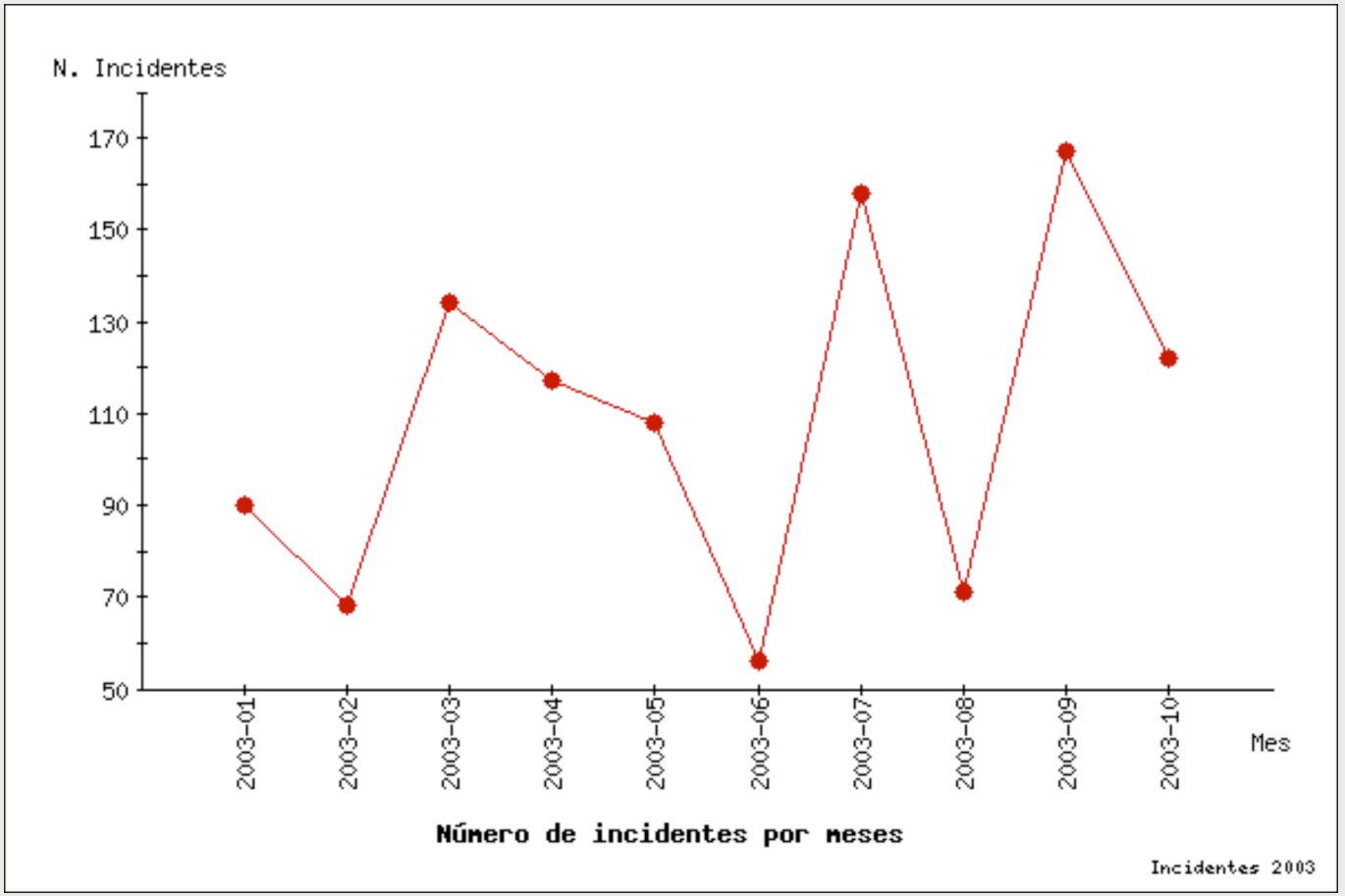
Informe de Incidentes
(Enero – Octubre 2003)

- Incidentes totales: 1091 **(7.22% menos que 2002)**
- Incidentes en el que están involucradas instituciones afiliadas: 1010 (92.57%). Periodo anterior 91%
  - Como origen: 622 (57%)
  - Como destino: 353 (32%)
  - Como origen-destino: 35 (3%)
- Incidentes ámbito internacional: 1013 (92.85%)
  - Origen internacional: 396 (36%)
  - Destino internacional: 617 (56%)
- Relacionados con infracción de copyright: 205 (Incremento 310%)
  - *Motion Picture Association (MPA)*: 92
  - *BaySTP, Inc (Paramount Picture Association)*: 58
  - *Vivendi Universal Entertainment*: 23
  - *Interactive Digital Software Association (IDSA)*: 22
  - *Business Software Alliance (BSA)*: 5
  - *Electronic Arts Inc. (EA), TITAN Media Inc., Sonic Solutions y Symantec Corporation*

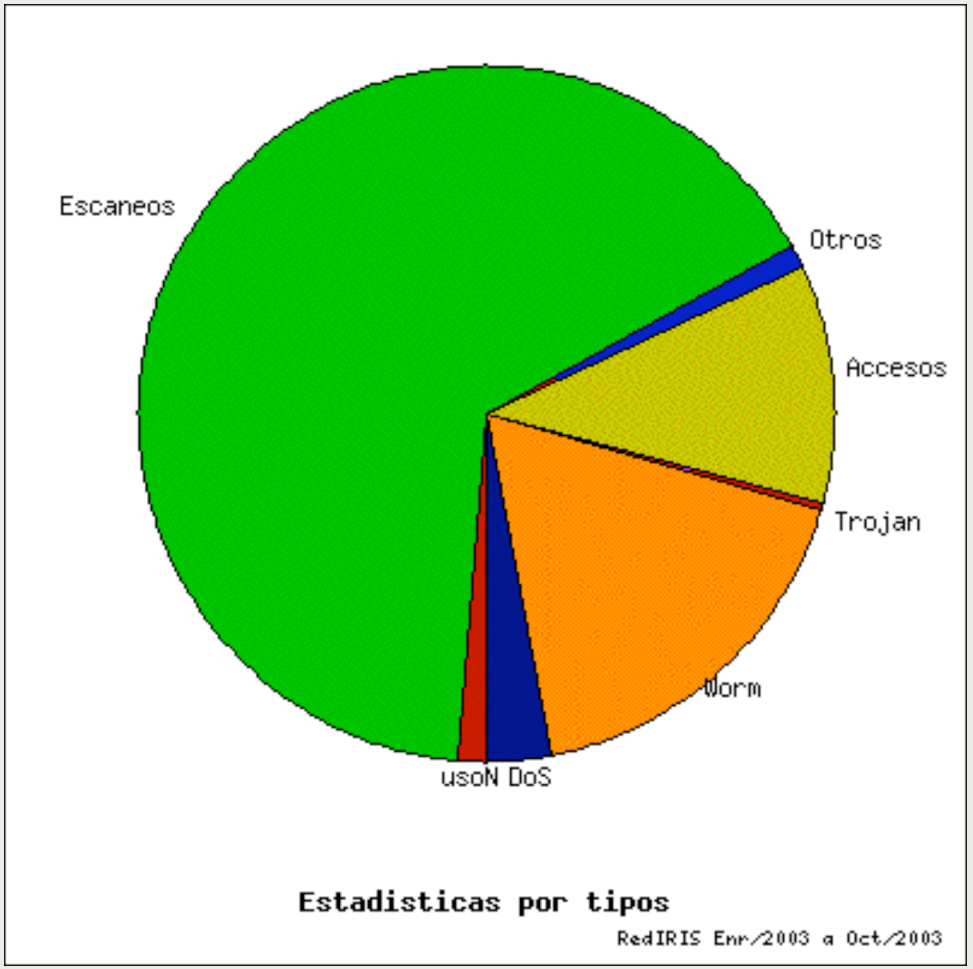
Informe de Incidentes
(Enero – Octubre 2003)



Informe de Incidentes
(Enero – Octubre 2003)



Informe de Incidentes
(Enero – Octubre 2003)



Informe de Incidentes
(Enero – Octubre 2003)

Tipo de incidentes	Nº Incidentes	%
Portscan	718	66%
Worm	191	18%
Accesos a cuentas privilegiadas	121	11%
DoS	33	3%
Uso no autorizado	14	1%
Otros	11	1%
Troyanos	3	0%

Informe de Incidentes
(Enero – Octubre 2003)

- Virus
  - Buena coordinación en las epidemias víricas del verano (Sobig, Mimail)
    - Alto impacto en el tráfico SMTP en los servidores institucionales
      - Estadísticas de RESACA Junio 2003

      Mensajes procesados: 2.331.906

      Virus encontrados: 25.972

      - Estadísticas de RESACA Agosto 2003 **(epidemia)**

      Mensajes procesados: 15.978.337

      Virus encontrados: 1.567.943

http://www.rediris.es/mail/resaca/

Informe de Incidentes
(Enero – Octubre 2003)

- Puertos más escaneados
  - netbios
    - 135/tcp-udp (*location service*)
    - 137/tcp-udp (*netbios name server*)
    - 138/tcp-udp (*netbios datagram service*)
    - 139/tcp-udp (*netbios session service*)
    - 445/tcp-udp (*microsoft-ds*)
  - http (80/tcp) (gusanos IIS, WebDAV)
  - 1434/udp, 1433/tcp (MS-SQL)
  - 1080/tcp (socks proxy, puerta trasera Bugbear)
  - 554/tcp (RTSP, Real Time Streaming Protocol)

  - DoS (ICPM flooding)

  Filtrar puertos en los routers de las organizaciones (entrada y salida) … if possible!! ☺

- Enero: Publicación del informe anual
  - http://www.rediris.es/cert/doc/informes/

Foros Nacionales
Subcomité técnico de seguridad en Espanix

- Evolución del foro ISPES (Coordinación de ISP en España)
  - Última reunión ISPEs Mayo 2002
    - Integración en Espanix
      - ESPX-MAIL
      - ESPX-CERT
      - ESPX-IPv6
- Octubre 2003: reunión para asentar las bases de los subcomités técnicos
  - Elaboración de un documento descriptivo para la junta directiva de Espanix
  - Inscripción tanto para miembros como para no miembros de Espanix
- Objetivos ESPX-CERT
  - Coordinación/Intercambio de experiencias
  - Definir acuerdos y acciones comunes
  - Establecer relaciones de confianza
  - Desarrollo de BCPs

Foros Internacionales

FIRST (Forum of Incidents Response and Security Teams)

http://www.first.org

- Iniciativa
  - *Request for Proposal: FIRST Incident Response and Forensics Guide*

    http://www.first.org/announcements/RFP/BPG/

- Eventos 2004
  - Dos *Technical Colloquiums* (restringidos a miembros del FIRST)
  - XVI Reunión Anual del FIRST (Budapest, Hungría, 13-18 Junio 2004)
    - Call for Papers (hasta 1 Dicembre)

      http://www.first.org/conference/2004/

Foros Internacionales
TERENA TF-CSIRT

http://www.terena.nl/tech/task-forces/tf-csirt/

- Novedades
  - Creación de un consorcio de equipos de seguridad dentro del TF-CSIRT para estandarizar y potenciar el uso del RT/RTIR como herramienta de gestión de incidentes, en colaboración con *Best Practical* (http://www.bestpractical.com/rtir/)
    - Investigar requerimientos para RTIR v2
    - Workshops RT/RTIR Madrid, 14 de Enero 2004
    - Colaboración en la creación de versiones futuras
  - Iniciativa para la elaboración de documentación sobre el objeto IRT de RIPE (*RIPE IRT object FAQ*, *RIPE IRT object - Technical HOWTO*)
    - http://www.dfn-cert.de/team/matho/irt-object/
    - *Trusted Introducer Service*
      - Disponibilidad de herramientas específicas para el uso de el objeto IRT
- Otras actividades relacionadas
  - *European Network and Information Security Agency (ENISA)* *eEuropa Action Plan 2003*
    - Agencia Europea para la seguridad de la información y las redes

Foros Internacionales
TERENA TF-CSIRT

- Otras actividades relacionadas (continuación)
  - Guía de legislación Europea de Seguridad
    - http://www.iaac.org.uk/csirt.htm
  - Proyectos Financiados por la CE
    - TRANSIT (*Training of Network Security Incident Teams Staff*, http://www.ist-transits.org/)
      - 25,26 Mayo. Alemania
    - EISPP (*Eurpean Information Security Promotion Programme*, http://www.eispp.org/)
      - Formato común para la generación de avisos de seguridad
      - Evolución: CEISNE (*Co-operative European Information Security Network of Expertise*) Entorno para compartir información sobre avisos de seguridad
    - eCSIRT.net (*European CSIRT Network*, http://www.ecsirt.net/)

- Eventos 2004
  - **11th TF-CSIRT meeting** - 15-16 Enero 2004, Madrid
  - **12th TF-CSIRT meeting** - 27-28 Mayo 2004, Hamburgo - Alemania
  - **13th TF-CSIRT meeting** - 23-24 Septiembre 2004, Valletta - Malta

eCSIRT.net
Justificación del proyecto

- No existe formación especifica en cuanto a administración de incidentes se refiere
  - El aprendizaje de esta tarea esta poco valorada
- **Avance lento de los estándares**
  - Los equipos de seguridad necesitan empezar desde niveles básicos
  - Carencia de soporte de herramientas, interfaces y bases de conocimiento para la administración
- Debilidades estratégicas
  - Los equipos no pueden acceder en la mayoría de los casos a la fuente del incidente

eCSIRT.Net
Descripción

- Origen
  - Equipos acreditados del *Trusted Introducer*
    - Comunidad establecida para pruebas reales
  - IODEF/IDMEF (desarrollos de la IETF)
    - Formatos de intercambio disponibles para incidentes
- Objetivos
  - **Mejorar** el intercambio de información relativa a incidentes
  - **Proporcionar** análisis y recopilación de los datos previamente compartidos
  - **Permitir** una colaboración eficiente y provechosa entre equipos
    - Estadísticas
    - Base de conocimiento compartida
    - Análisis de tendencias, alertas tempranas, ...

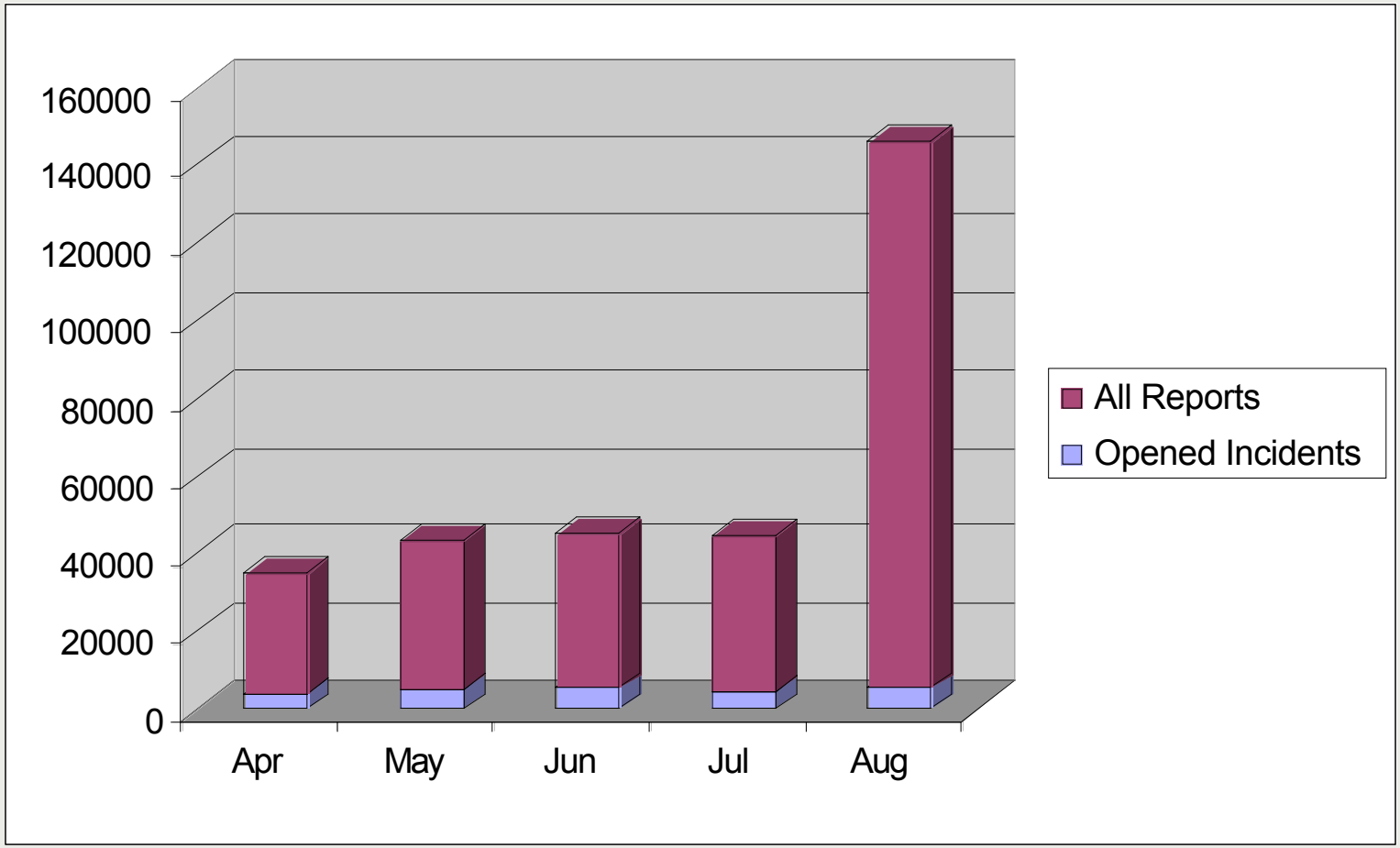
eCSIRT.net
Integrantes del Proyecto

- Participantes
  - CERT-POLSKA / NASK — Polonia
  - DN-CERT — Alemania
  - DK-CERT / UNI-C — Dinamarca
  - GARRNET-CERT / INFN — Italia
  - IRIS-CERT / RedIRIS — España
  - JANET-CERT / UKERNA — Reino Unido
  - Le CERT Renater — Francia
  - STELVIO bv — Países Bajos
  - PRESECURE Consulting GmbH — Alemania
- Colaboradores
  - CERT/CC — USA
  - CERT-NL (Surfnet-CERT) — Países Bajos
  - JP-CERT/CC — Japón

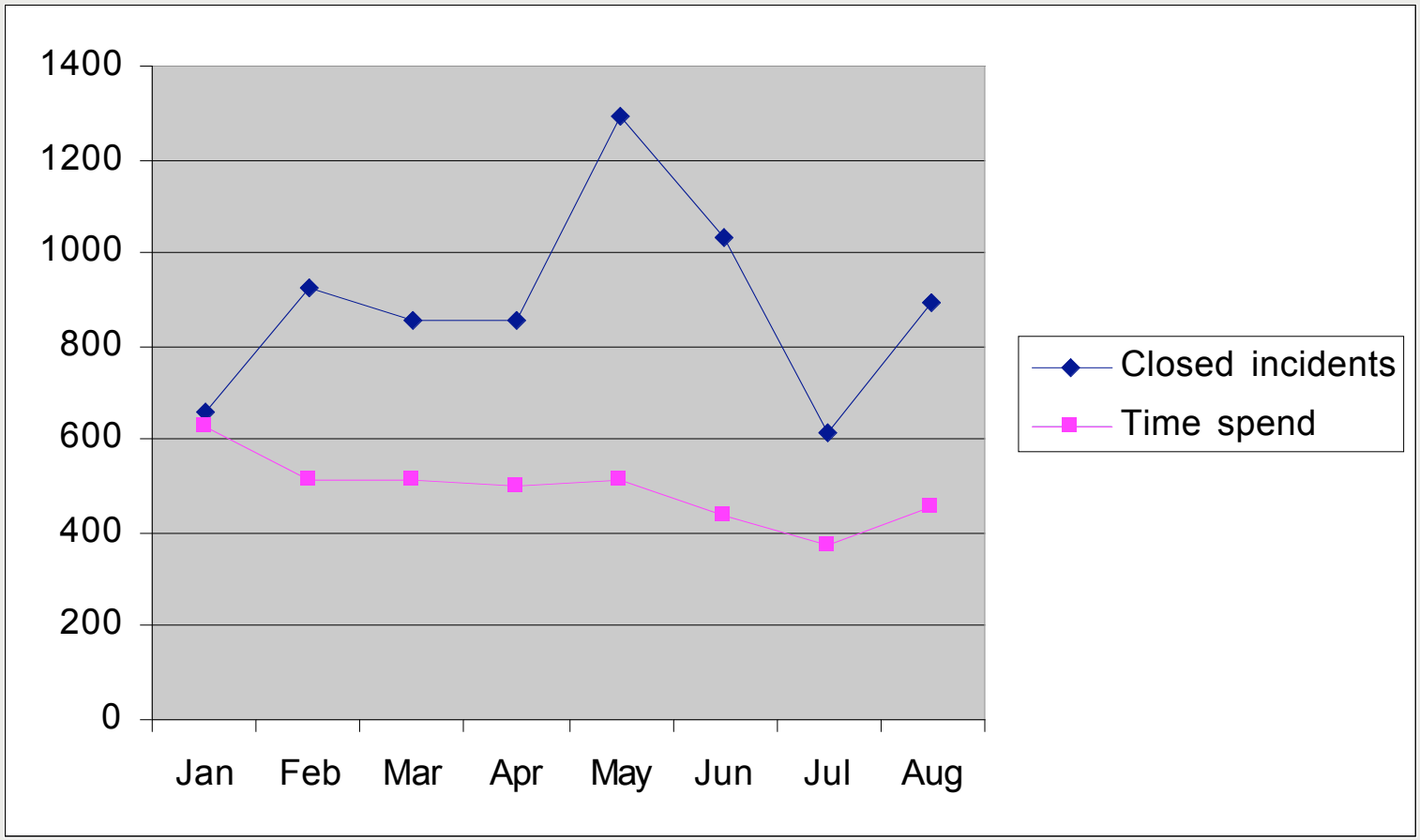
eCSIRT.net
Fases del Proyecto

- WP1. Administración del proyecto
- **WP2. Definición de un lenguaje común** (especificación, adaptación e integración de las técnicas disponibles, así como el desarrollo de un marco de trabajo común para permitir y facilitar el trabajo futuro)
  - Definición de un código de conducta
  - Basado IODEF/IDMEF (tanto para el intercambio como para el almacenamiento de la información)
- **WP3. Uso del lenguaje común**
  - Evaluación y adaptación de las herramientas existentes para el uso del lenguaje común
- **WP4. Obtención de estadísticas**
  - Recolección de estadísticas sobre incidentes de los miembros del proyecto y su publicación usando un formato común (estadísticas privadas y públicas)
    - De carga de trabajo y recursos empleados
    - De incidentes
    - Del nivel de peligro de los sistemas conectados a Internet (red de sensores)
- **WP5. Función de alerta (alertas temprana y de emergencia)**
  - Generación y distribución segura de advertencias y alertas a los miembros del proyecto
- WP6. Valoración y evaluación de resultados
- WP7. Publicación de resultados

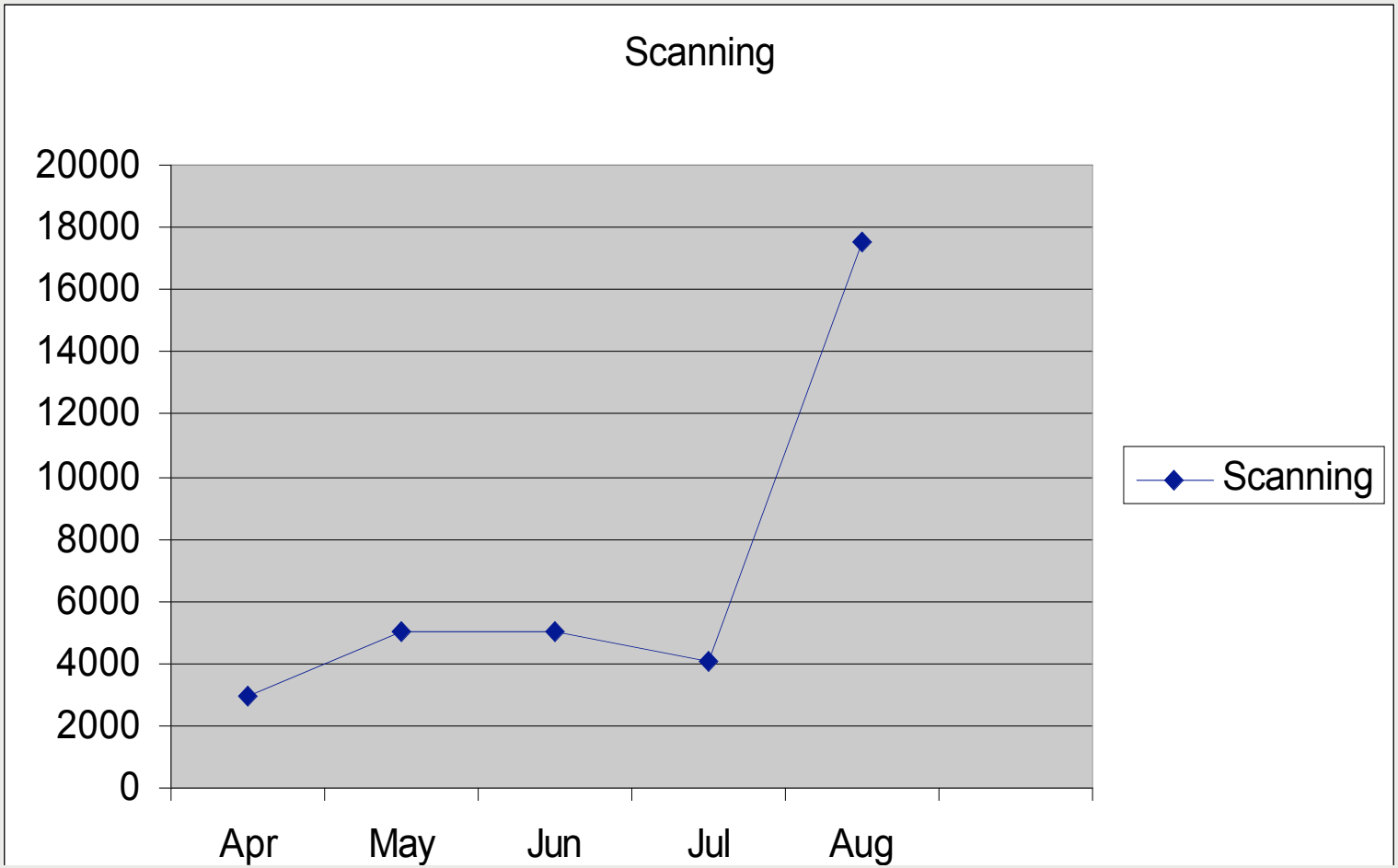
eCSIRT.net
Estadísticas Tipo 1 (5 Equipos)



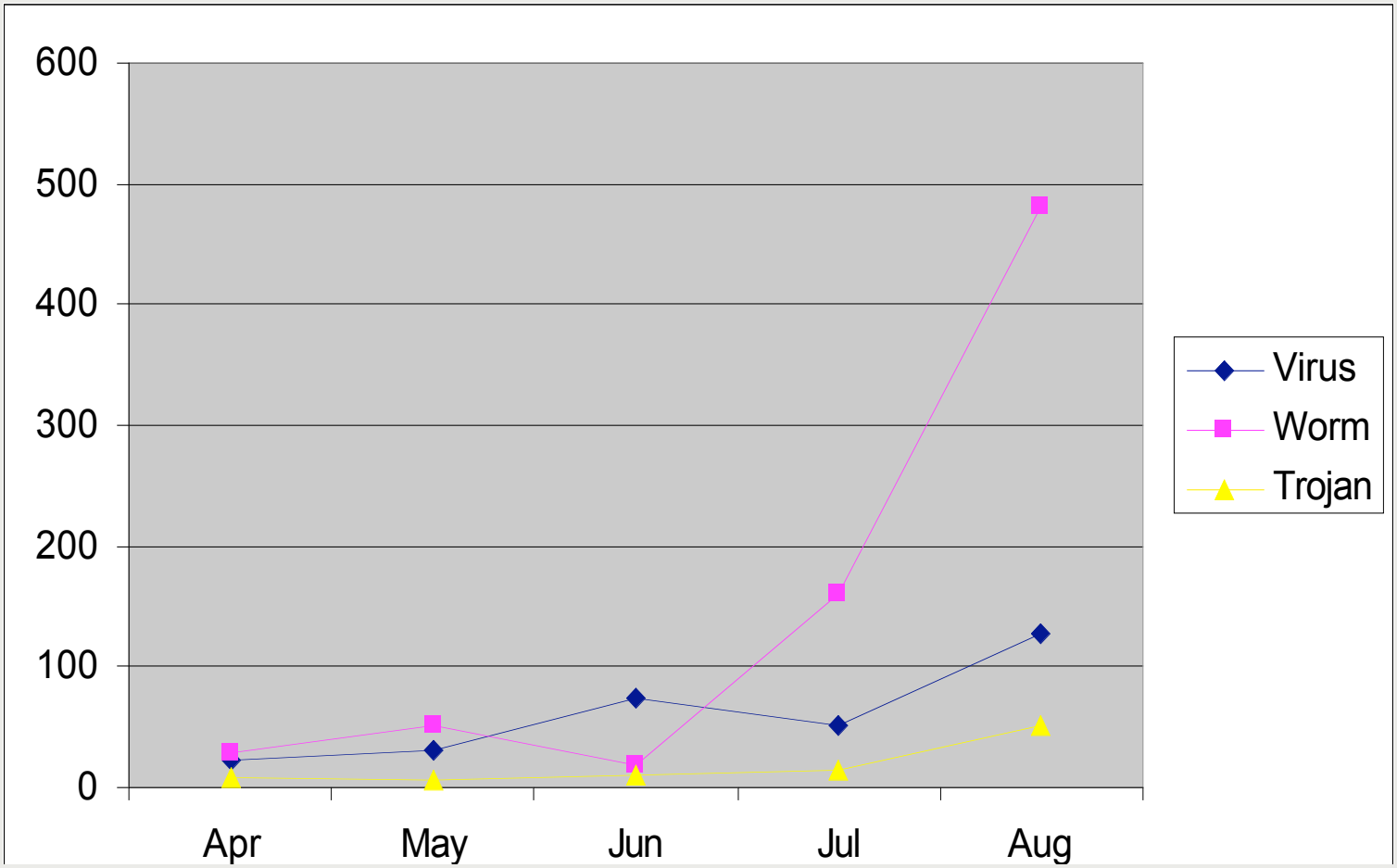
eCSIRT.net
Estadísticas Tipo 1 (5 Equipos)



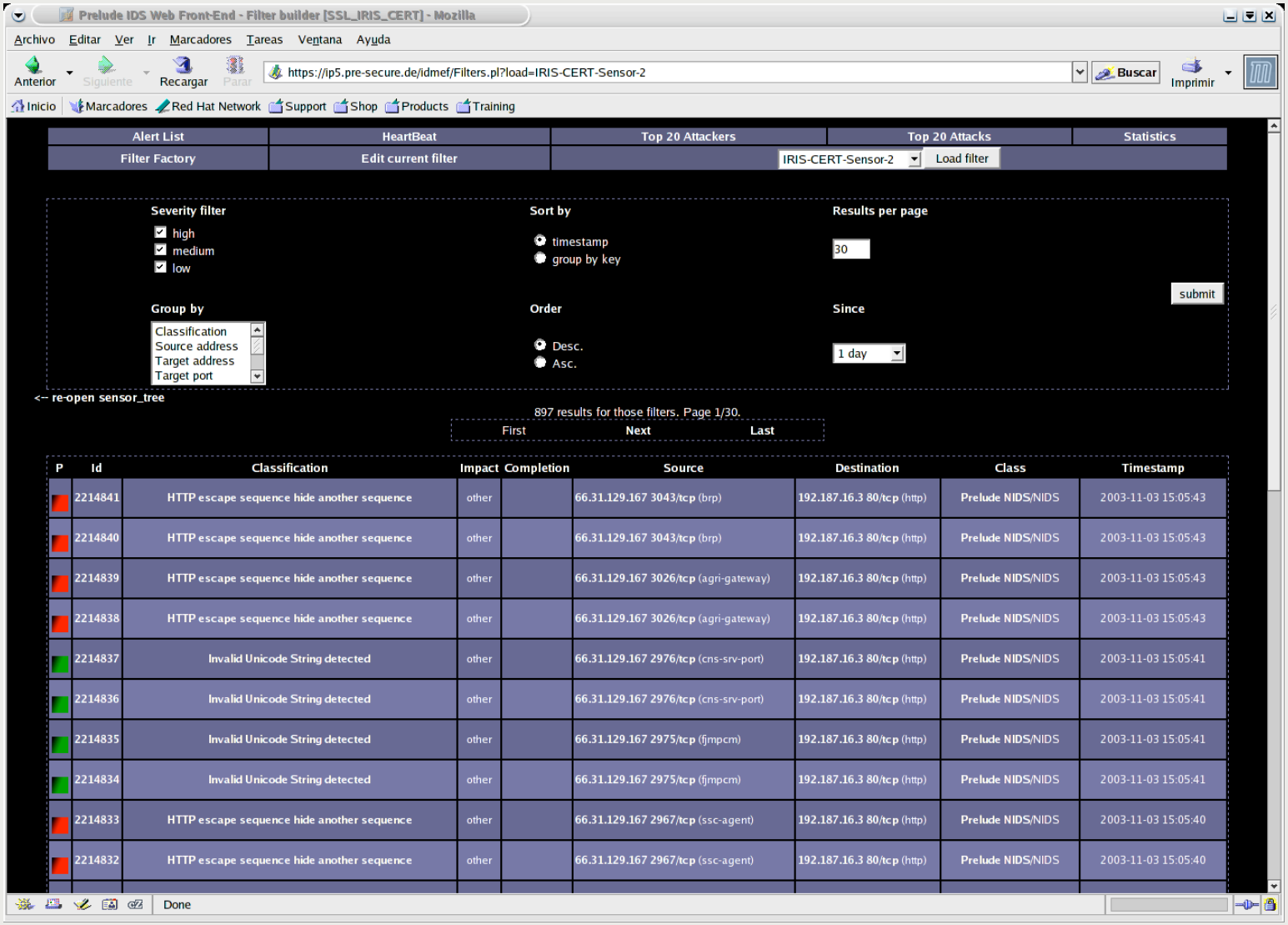
eCSIRT.net
Estadísticas Tipo 2 (3 Equipos)



eCSIRT.net
Estadísticas Tipo 2 (3 Equipos)



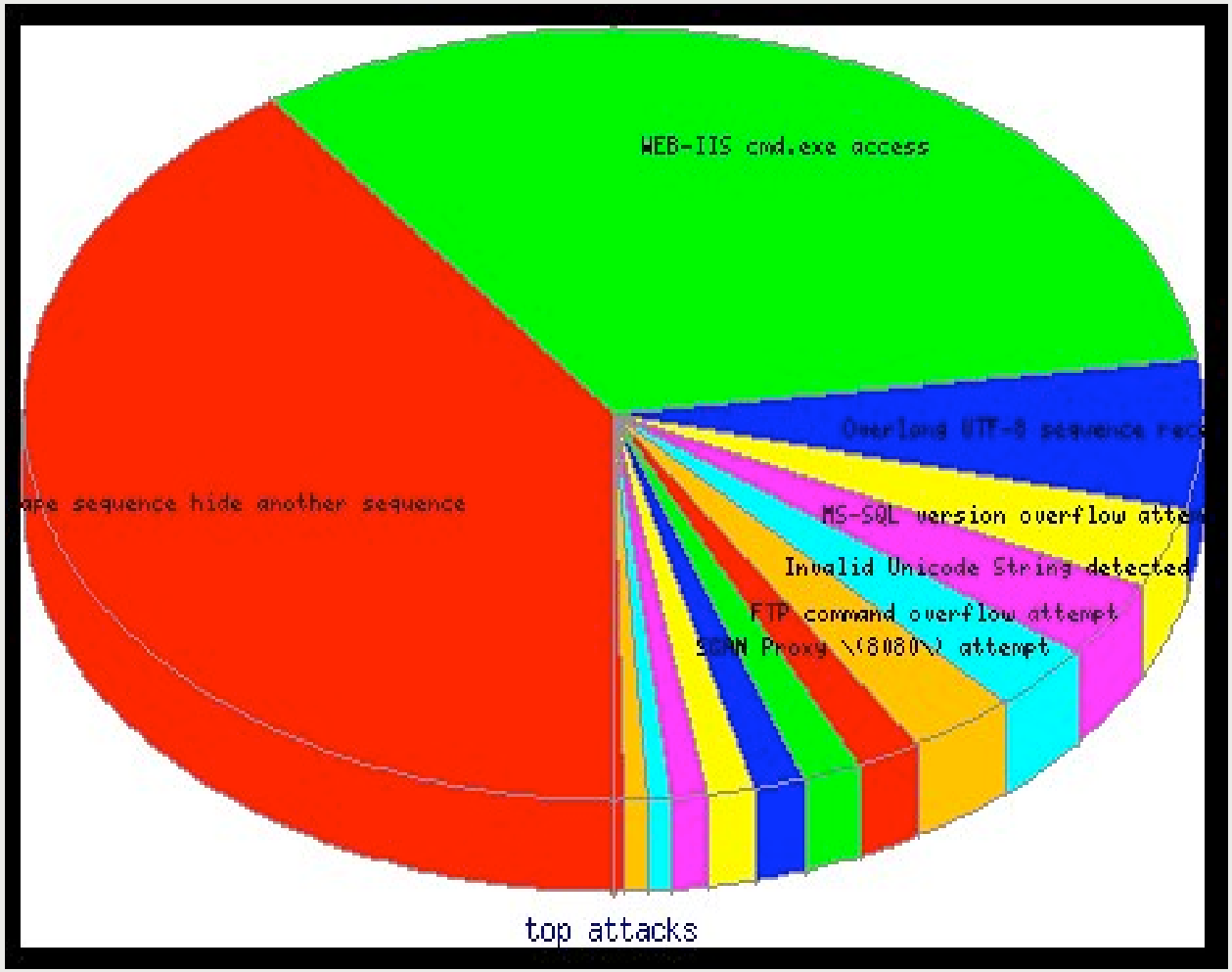
eCSIRT.net
Estadísticas de Acceso (Tipo 3) (I)



eCSIRT.net
Estadísticas de Acceso (Tipo 3) (II)

AttackNb	Attack name
250	HTTP escape sequence hide another sequence
202	WEB-IIS cmd.exe access
39	Overlong UTF-8 sequence received
21	MS-SQL version overflow attempt
20	Invalid Unicode String detected
18	FTP command overflow attempt
18	SCAN Proxy \(8080\) attempt
11	ICMP PING NMAP
10	WEB-IIS ..\.. access
9	SCAN Squid Proxy attempt
8	WEB-IIS nsiislog.dll access
6	ICMP PING CyberKit 2.2 Windows
4	ICMP superscan echo
4	WEB-IIS CodeRed v2 root.exe access
2	ICMP Destination Unreachable (Communication Administratively Prohibited)

eCSIRT.net
Estadísticas de Acceso (Tipo 3) (III)



eCSIRT.net
Estadísticas: Ataques por sensor

```
$host> ./attackers_seen_per_sensor.pl -B

# 96240 attacks exist in database.
# alerts from 6 different sensors exist.
# alerts from 13332 different hosts exist.
13012 attacking hosts seen by 1 sensors.
  242 attacking hosts seen by 2 sensors.
   49 attacking hosts seen by 3 sensors.
   23 attacking hosts seen by 4 sensors.
    1 attacking hosts seen by 5 sensors.
    5 attacking hosts seen by 6 sensors.
```

eCSIRT.net
Estadísticas: Ataques por máquina

```
$host> ./different_attacks_per_host.pl -B

10075 hosts seen using  1 different attacks.
 1777 hosts seen using  2 different attacks.
  859 hosts seen using  3 different attacks.
   71 hosts seen using  4 different attacks.
  514 hosts seen using  5 different attacks.
   18 hosts seen using  6 different attacks.
    9 hosts seen using  7 different attacks.
    3 hosts seen using  9 different attacks.
    2 hosts seen using 10 different attacks.
    2 hosts seen using 11 different attacks.
    2 hosts seen using 14 different attacks.
```

Otras actividades
Objeto IRT-IRIS-CERT

irt: **IRT-IRIS-CERT**
address: IRIS-CERT
address: Centro de Comunicaciones CSIC-RedIRIS
address: Serrano, 142
address: E-28006 Madrid
address: Spain
phone: +34 91 585 5150
fax-no: +34 91 585 5146
e-mail: cert@rediris.es
signature: PGPKEY-88A17FF5
encryption: PGPKEY-88A17FF5
admin-c: TI123-RIPE
tech-c: TI123-RIPE
auth: PGPKEY-88A17FF5
remarks: Emergency telephonenumber +34 915855150 (GMT+1/GMT+2 with DST)
remarks: http://www.trusted-introducer.org/teams/iris-cert.html
remarks: This is an accredited IRT (level 2)
irt-nfy: cert@rediris.es
notify: tiirt@stelvio.nl
notify: cert@rediris.es
mnt-by: TRUSTED-INTRODUCER-MNT
changed: gert-henk.bakker@stelvio.nl 20030310
source: RIPE

- Todos los rangos enrutados por RedIRIS han sido enlazados con el objeto IRT-IRIS-CERT

Otras actividades
Reto análisis forense

- Objetivo
  - Fomentar la formación en análisis forense de los administradores y responsables de seguridad de las instituciones afiliadas
- Cuando
  - Antes de finales de año
- Qué hay que hacer
  - Analizar una máquina previamente atacada (perteneciente a la red de máquinas trampa de RedIRIS) y contestar a unas preguntas relacionadas
- Cómo participar
  - http://www.rediris.es/cert/ped/reto/

Otras actividades
Jornadas USC (Abril-Mayo)

- ¡¡Gracias a la Universidad de Santiago de Compostela!!
- Hay que decidir todavía el contenido y estructura del workshop (creación de un comité de programa)
  - TRANSIT. Dividido en 5 módulos
    - Organizacional
    - Técnico
    - Operacional
    - Legal
    - Generación de avisos
- ¡¡Se necesitan voluntarios para impartir las clases!!

Próximos eventos

- Workshop RT/RTIR. 14 Enero 2004, Madrid
- XI reunión TF-CSIRT. 15-16 Enero 2004, Madrid
- *ISP Abuse Management Forum*
  - Foro para el establecimiento de una red de comunicación europea entre ISPs para el manejo de incidentes de abuse
  - http://www.ispforum.net/

¡¡¡¡Muchas gracias!!!!