Grupo de Trabajo IRIS-CERT

IRIS-CERT ,RedIRIS

26 de Octubre 2004

Indices

Informe de actividades

- Reuniones y grupos de trabajo
- Estadísticas de incidentes de Seguridad
- Incidencias más destacadas.
  - botnets
- Algunos problemas en la coordinación
- Otras cosas

Ataques en IPv6

Mesa redonda

- **Grupo de coordinación Europeo de Seguridad , no limitado a redes académicas.**
- **3 Reuniones anuales, organizamos la reunión de Enero en Madrid**

Acciones:

- ❑ Herramienta de Gestión de incidentes RTIR
- ❑ ECSIRT.net
  - Red de Sensores
  - Normalización de estadísticas
  - Pruebas de IODEF
- ❑ Reunión de grupos de abuse

Organización de cursos transit sobre la creación de grupos de seguridad

JR2:

Grupo dentro de Gean sobre seguridad dentro de la futura red Gigabit académica Europea. (Gean 2)

- Protección de los elementos de infraestructura de red.
- Construcción de elementos de seguridad
  - Monitorización de tráfico en base a flujos
  - Detección de ataques (DDOS) dentro de la Gean2
- Infraestucturas de coordinación de incidentes de seguridad.

Básicamente reuniones técnicas,

- Publicación de las ponencias (Congreso) en Febrero de este año.

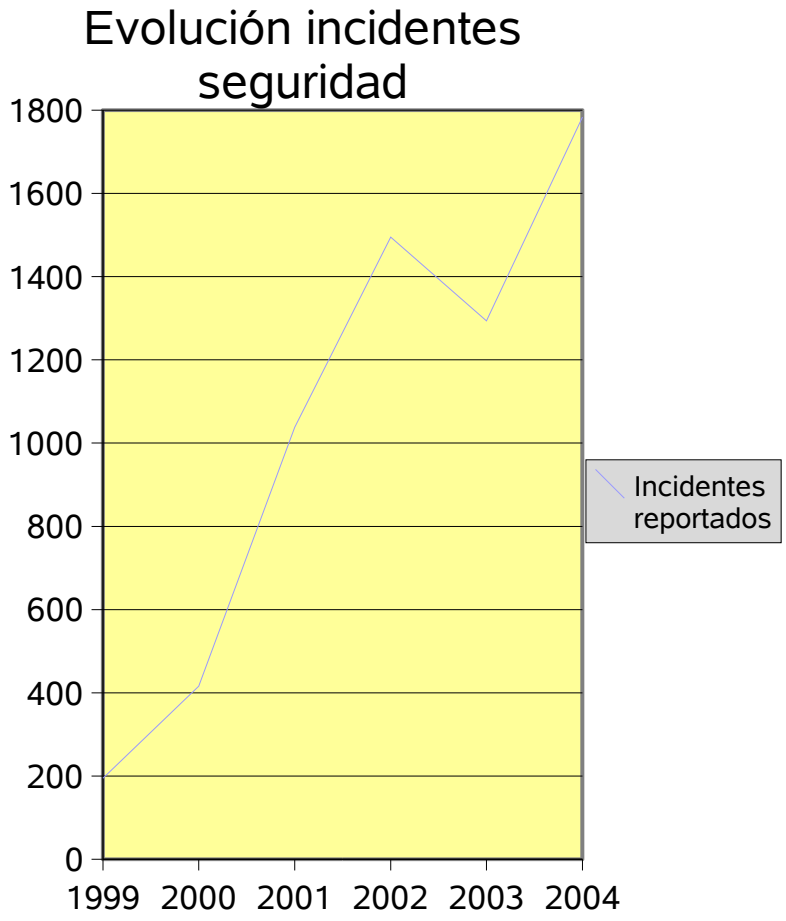
Novedades :

- Análisis forense:
  - W Venema: Herramienta de análisis de sistemas de ficheros de log (ext3, reiserfs, etc).
- Detección de intrusiones
  - Documentación sobre rootkis en Unix y Windows

Reto Análisis Forense

- Reto/concurso para analizar una máquina Linux ataque
- Objetivos:
  - Fomentar el conocimiento de técnicas de Análisis Digital.
  - Obtener documentación de referencia en Castellano sobre el reto
- Resultados:
  - 14 trabajos presentados
  - Alto nivel de todos los trabajos
  - Algunos problemas de organización ;-)
- Documentación disponible en las páginas del grupo de seguridad
- Mesa redonda ahora después

Evolución incidentes por años



Sigue aumentando el número de incidentes reportados cada año.

- Los cambios en los procedimientos de gestión de incidentes y herramientas hacen que este aumento no aparezca directamente reflejados.
- Modificaciónde tendencia sobre el tipo de objetivo: usuario final con Windows.
- Pruebas de aviso sobre máquinas posiblemente comprometidas para evitar la propagación de ataques

Herramienta gestion de incidentes

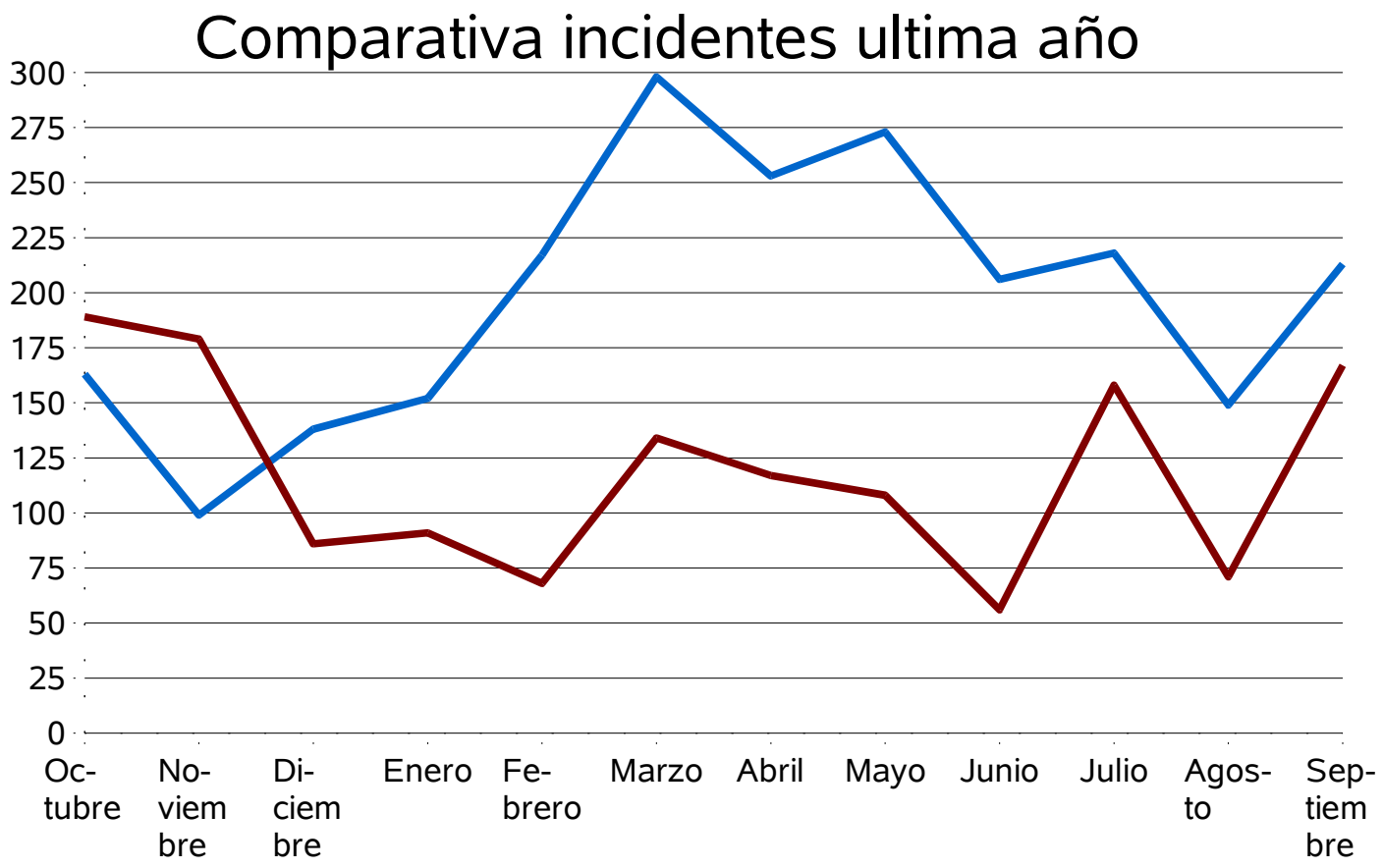
Antes:

- Mismo código para todo el intercambio de información relativo a un incidente.
- A Nivel de operación , se procuraba que un incidente solamente involucrara una organización
- Varios tipos de correos sin incidente: Copyright, preguntas, notificaciones de ISP (menos 10%)
- Envío de los mensajes directamente desde agente de correo.
- Control manual de fechas

Ahora

- Códigos distintos (incident report, incidentes , investigaciones y filtros)
- Posibilidad de controlar en un mismo incidente problemas en varios equipos de distintas organizaciones.
- Agrupación en algunas categorias de uno interno los eventos que corresponden a asuntos de copyright, preguntas, etc.
- Envío de mensajes desde la herramienta (no personalización)
- Control automático de fechas

Incidentes por meses



Azul: 2004

Rojo: 2003

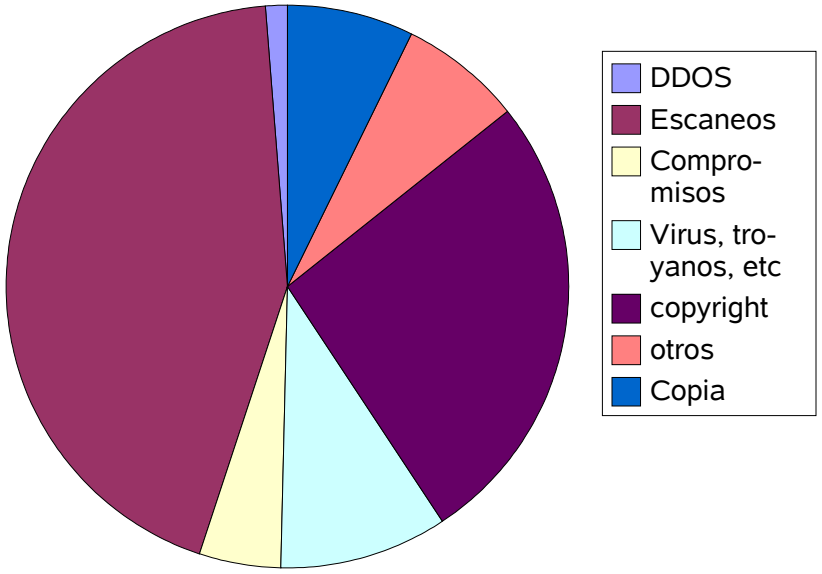
Algunos comentarios sobre los incidentes:

- ¿Tiene incidencia las Jornadas en el número de incidentes ?
- Se aprecia el incremento de incidentes en Marzo- Abril debido a las oleadas de Gusanos de Windows.
- Muy pocos incidentes son detectados en las organizaciones, gran parte de ellos llega en base a quejas externas.
- Aumenta el número de scripts automáticos de detección de escaneos:
  - DSHIELD, http://www.dshield.org (pocos)
  - Mynetwatchman http://www.mynetwatchman.com
- Problema del usuario final : Falta información, pantallazos, etc.

Tipos de ataques

Estadísticas desde Mayo a Octubre

- Más de 1300 incidentes
- No todos los "incidentes" tiene la misma importancia:
  - Copyright
  - Copia
- Gran parte de los escaneos deben ser debidos a gusanos, etc, pero no tenemos más información.
- DDOS: Algunos ataques no son tales.



Ataques más frecuentes

Ataques fuerza Bruta SSH

Junio:

- Intentos de acceso usuario “test” /pwd test vía ssh en sistemas Linux/Unix.
- Pocos equipos comprometidos
- Password muy débiles
- Exploit locales (núcleo) para acceder después al equipo.
- Herramienta disponible en varios foros y listas de distribución

Octubre:

- Lista creciente de usuarios , no solo usuarios por defecto.
- Diversas pruebas/ combinaciones con usuarios.
- Se detectan varios equipos en la red académica atacando mediante diversas herramientas.

BotNets

- La mayoria de los incidentes reportados parecen tener como origen equipos formando parte de botnets.
- Las quejas recibidas muchas veces no permiten determinar exactamente que es lo que esta sucediendo en el equipo
  - ¿Gusano de correo electrónico ?,
  - ¿Atacante individual ?
  - Ataques automáticos (bots)
- Casi exclusivamente los ataques son a al plataforma Windows.

Windows, ¿El sistema más atacado ?

Bastan tes mejoras en el sistema Operativo a nivel de seguridad

- Muchos usuarios finales no actualizan equipo.
- Es necesario filtrar en salida y entrada los puertos empleados por estos sistemas.
  - 135-139/TCP, 445/TCP, 5000/TCP
  - 1433/TCP 1434/UDP,
  - NO todas las instituciones tienen filtrado estos puertos de entrada
  - Menos filtros de salida, permiten la salida de los ataques.
- Portátiles y VPNs propagan dentro de organizaciones “seguras” los equipos infectados.

1433/TCP: servidores MS-SQL

- Diversas vulnerabilidades en este servidor , debidas muchas veces a password de administrador vulnerable.
- Existencia de gusanos propagandose en este puerto.
- Hace unos años estos ataques eran empleados muchas veces para la instalación de servidores FTP

- Detección de muchos equipos escaneando este puerto
- Problemas:
  - Escasa información recibida como respuesta
  - La información recibida indica muchas veces ataques “manuales”, no debidos a gusanos/bots/virus

Falta de respuesta sobre el estado de los incidentes:

- ¿Se ha recibido el correo ?
- ¿Se ha podido solucionar el problema ?

¿Ya solucionado ?

- Muchas veces esta es la única información sobre que ha sucedido en un incidente.
- Después de insistir dos o más veces sobre el problema.
  - ¿Se trataba de un virus ?, ¿ botnet ?
  - Un ataqué manual para instalar un servidor Warez ?
- Dificultad para conocer desde IRIS-CERT , que tipo de ataque se esta produciendo y que tendencias hay.
- Aumento del tiempo de trabajo para un incidente (sobre todo si no se responde)

Otras cosas

Otras cosas

Día de la seguridad informática

- Promovido por la IEEE
- Objetivo concienciar a los usuarios de los problemas de seguridad, en un sentido amplio:
  - Antivirus y actualizaciones
  - Copias de seguridad
  - ....
- A nivel castellano sobre todo en México
  - Día de la Seguridad en Computo
  - www.disc.unam.mx
- Este año esta previsto celebrarlo el día 8 de Diciembre 2004

¿Ruegos ?,

....

¿Preguntas ?

....

¿Comentarios ?