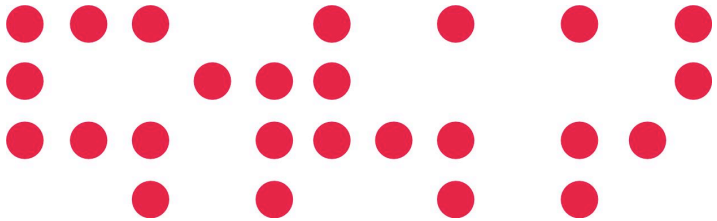
Actualidad Seguridad
ASTIRIS

Carlos Fuentes/Chelo Malagón
RedIRIS, IRIS-CERT

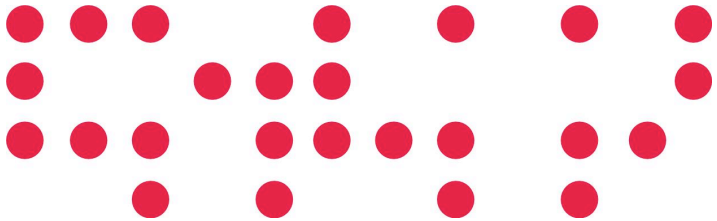
Alcalá de Henares, 18 de Noviembre de 2006

Agenda

- Incidentes
  - Casos a destacar
    - Vulnerabilidad DNS
    - Ataques wifi/eduroam
    - Ataques de phishing
  - Política de filtrado
  - Puntos de contacto del CERT
- Repaso iniciativas
  - Grid CERT
  - Sellado Digital de Tiempos
  - Recolección evidencias con Rpier
  - GT-REQSEG: Iniciativa SIRA
- Nuevas iniciativas
  - NetReflex (Detección anomalias)
  - DNS Blackholeing
- Cursos y eventos

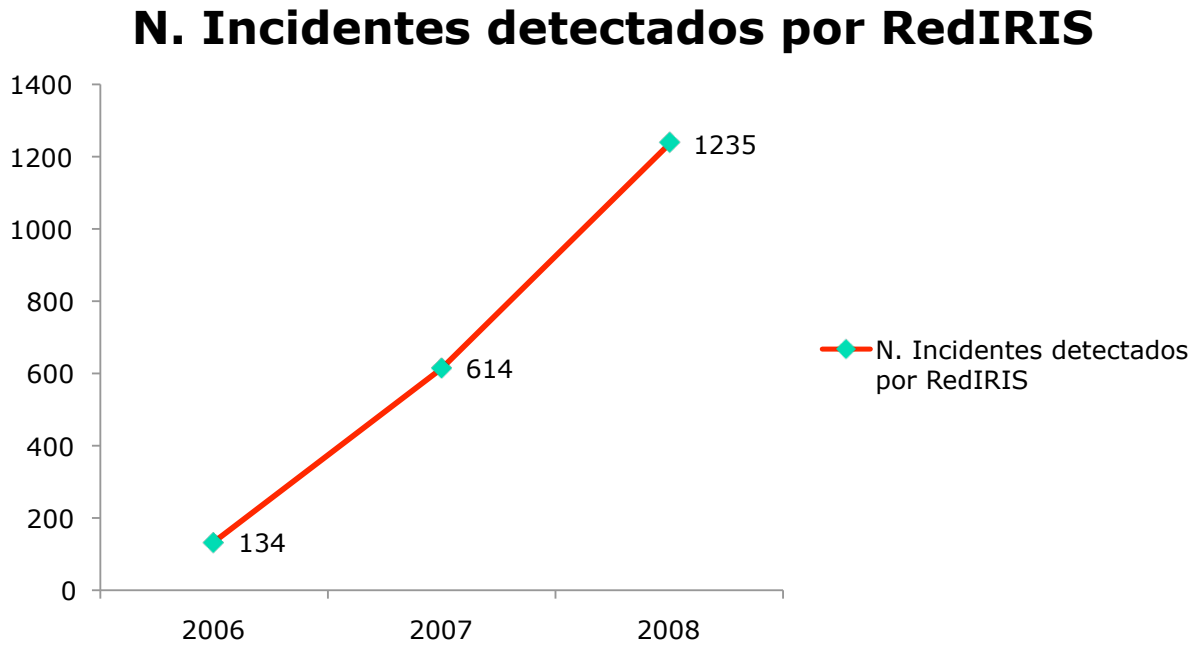


Sobre Incidentes



Algunos datos del CERT

- Uso de herramienta de detección
  - Plugins NFSEN
  - DNS blackholeing
  - LogSufer
  - Spamtoso

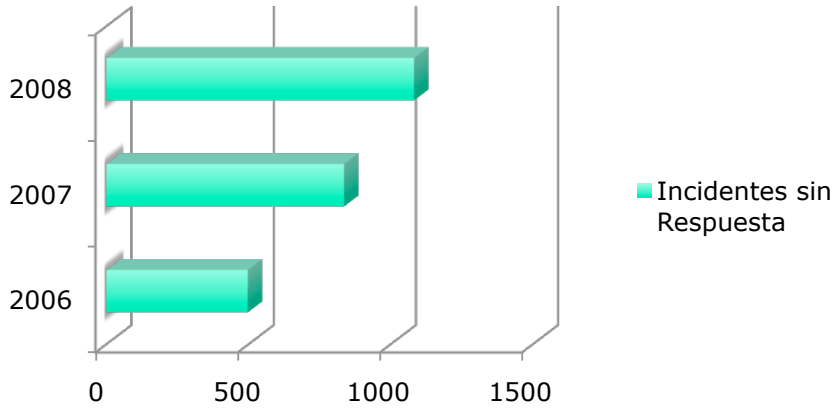


IRIS-CERT <cert@rediris.es>

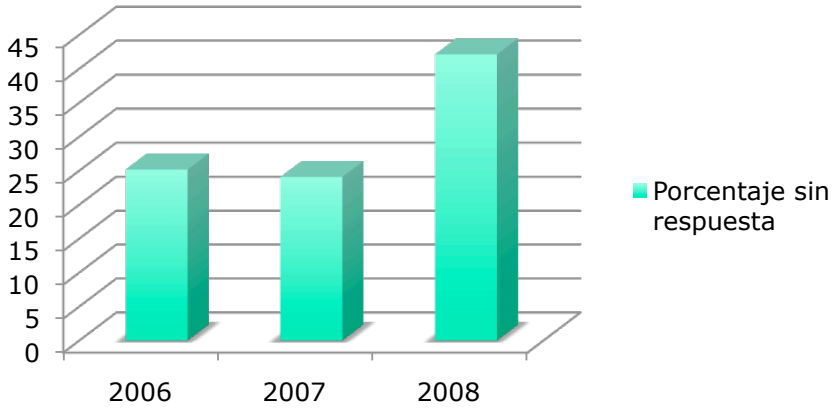
Algunos datos del CERT (II)

- Seguimos con el mismo problema:
  - No hay respuesta
  - ¿por qué? ¿existe algún problema?

Incidentes sin Respuesta

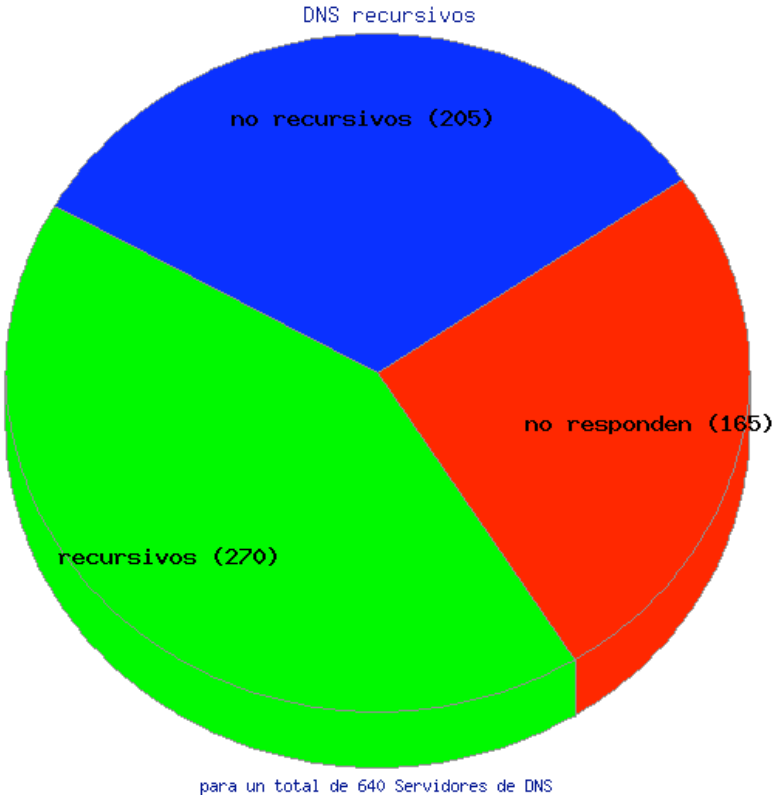


Porcentaje sin respuesta



Sobre vulnerabilidad DNS

- Estado DNS recursivos en RedIRIS. Marzo 2006



- Estado DNS recursivos en RedIRIS. Noviembre 2008

Incidentes relacionados con wifi/eduroam

- Pocas incidencias reportadas
  - eduroam ➔ usuarios localizados y avisados
    - Política movilidad de la iniciativa eduroam ES
      - http://www.eduroam.es/politica.es.php
    - Comunicar incidencias
      - eduroam@rediris.es y cert@rediris.es
  - wifis abiertas
    - Servidor NAT de gestión de tráfico Wifi o de salida general del centro
    - En la mayoría de los casos no se pudo localizar al usuario
      - Registro de autenticación/acceso a la red. Detección/registro de direcciones MAC
        - Incubadora/notificación del usuario la próxima vez que se conecte a la Web
      - Filtro de salida (HTTP+SMTP)
        - No soluciona el problema de conexiones a repositorios de keyloggers y otros malware
          - DNS Balckholeing (http://www.rediris.es/cert/proyectos/dns-black/)
  - Tipo de quejas recibidas
    - Conexiones a repositorios de Keylogger, a C&C de botnets, spyware, escaneos….

Ataques de Phishing verano 2008 (I)

- Contra usuarios de las Universidades
  - Mensajes mal redactados pero ataque dirigido
  - Usuario/password de webmail ➔ SPAM, suplantación de identidad
    - Pocas cuentas comprometidas por Universidad ➔ Utilización extensiva de dichas cuentas (SPAM)
  - "Reply to:" reencaminado cuentas gratuitas
  - Gran variedad de IPs orígenes
- Acciones
  - Alerta a los usuarios
  - Notificación responsables IPs origen y proveedores de correo gratuito
  - Borrado del mensaje en cuentas sin leer
  - Bloqueos de acceso a cuentas webmail comprometidas
  - Inclusión de IPs en listas negras
  - Bloqueo en salida de los "Reply To:"
  - Mayor control en el correo entrante/saliente
  - Control de flujo de envío de mensajes

Ataques de Phishing verano 2008 (II)

Subject: Verificar y actualizar su Universidad e-mail
Date: Thu, 07 Aug 2008 20:23:37 +0100
To: "undisclosed-recipients:"@parker.sim. .es [lookup host]
From: Messaging Center <blanche@3web.net> [lookup email] [lookup "3web.net"]

Estimado Universidad los usuarios,

Este mensaje es de la Universidad , centro de mensajer_a
para todos Universidad d users.We [lookup host] correo electr_nico son
actualmente la mejora de nuestra base de datos y e-mail centro. Estamos
suprimiendo todos los no utilizados .es [lookup host] correo electr_nico, Usted est_
obligado a verificar y actualizar su mensaje de correo electr_nico confirmando
su identidad. Esto evitar_ que su direcci_n de correo electr_nico de concluidos
durante este ejercicio. Con el fin de confirmar la identidad de correo
electr_nico que usted, usted es para proporcionar los siguientes datos;

Confirmar su identidad por debajo de correo electr_nico

Nombre :.....
Apellido :.....
Email Nombre de usuario: .....
E-mail Contrase_a: .....

_Advertencia! .es [lookup host] correo electr_nico
Email usuario que se niega a verificar y, posteriormente, actualizar su correo
electr_nico dentro de los siete d_as de haber recibido esta advertencia perder_
su correo electr_nico
permanentemente.

Gracias por utilizar nevada.edu [lookup host] correo electr_nico!
Advertencia C_digo: VX2G99AAJ

Gracias,
Universidad

Copyright _ 2008, Universidad de Madrid todos los derechos
reservados.

3webLD gives you the lowest long distance rates out there...Canada calling
as low as 2 cents/min...U.S. as low as 4 cents/min...visit www.get3web.com [lookup host] for
details

"
De: Senior Manager of Fraud/Crime Management
[mailto:mr.oscarmartinez@gmail.com [lookup email] [lookup "gmail.com"]]
Enviado el: sábado, 19 de julio de 2008 11:33
Para: undisclosed-recipients:
Asunto: Estimados usuarios de correo web de ,

Estimados usuarios de correo web de ,
Este mensaje es UNVERSIDAD de la) (Anti-Scam
centro de mensajes de correo web los usuarios. en estos momentos estamos
actualizando nuestra base de datos y e-mail centro. Estamos la
cancelación de todos los no utilizados Webmail cuenta para evitar
actividades fraudulentas y estafa en Internet. Usted está obligado a
verificar de inmediato y actualizar su dirección de e-mail confirmando
tu e-mail identidad. Esto protegerá a tu e-mail de concluidos durante
este ejercicio. Con el fin de confirmar la actualización de su dirección
de correo electrónico, Usted deberá proporcionar los siguientes datos;
Confirme su dirección de e-mail identidad
Registro Nombre:
Apellido:
El nombre de usuario e-mail:
E-mail Contraseña:
¡Atención! UNVERSIDAD) (Webmail usuario que se
niega a verificar y actualizar Sus e-mail dentro de los siete días de
recibir este aviso, su dirección de correo electrónico se dará por
terminado definitivamente.
Recuerdos,
Mr.Oscar Martínez
Senior Manager de fraude o de gestión de la delincuencia
Correo electrónico: mr.oscarmartinez@gmail.com [lookup email] [lookup "gmail.com"]

=re>No virus found in this incoming message. Checked by AVG -
http://www.avg.com [lookup "://www.avg."] Version: 8.0.138 / Virus Database: 270.5.2/1561 -
Release Date: 18/07/2008 18:35

"

Saludos.

Política de gestión de incidentes IRIS-CERT

- Política de Gestión de Incidentes:
  - http://www.rediris.es/cert/procinci.es.html
  - NO es nueva
  - Procedimiento de actuación ante incidencias

- Puntos de contacto
  - Proceso de validación en próxima semana
  - Objetivo
    - PERs verifiquen y validen los puntos de contacto
    - Evitar contactar con personas inadecuadas

Repaso Iniciativas

- EGEE-III
  - CSIRT para SWE (España y Portugal)
  - De turno a nivel EGEE cada dos meses
  - Miembros del OSCT (Operational Security Coordination Team)
    - Incident Response Activity
    - Service Security Challange
  - Estrechar vinculos entre NREN CERTs y OSCT
- CSIRT para NGI Española
  - Modelo propuesto por RedIRIS desde SWE

- Recolección de evidencias utilizando Rpier
  - 20-30 instituciones
  - Análisis en función de disponibilidad
- Grupo de Trabajo Requerimientos de Seguridad (GT-REQSEG)
  - Iniciativa SIRA (Seguridad Informática en la Red Académica)
  - Más a continuación …
- Sellado Digital de Tiempos
  - GT sobre requisitos de un servicio de sellado digital de tiempo sin validez legal

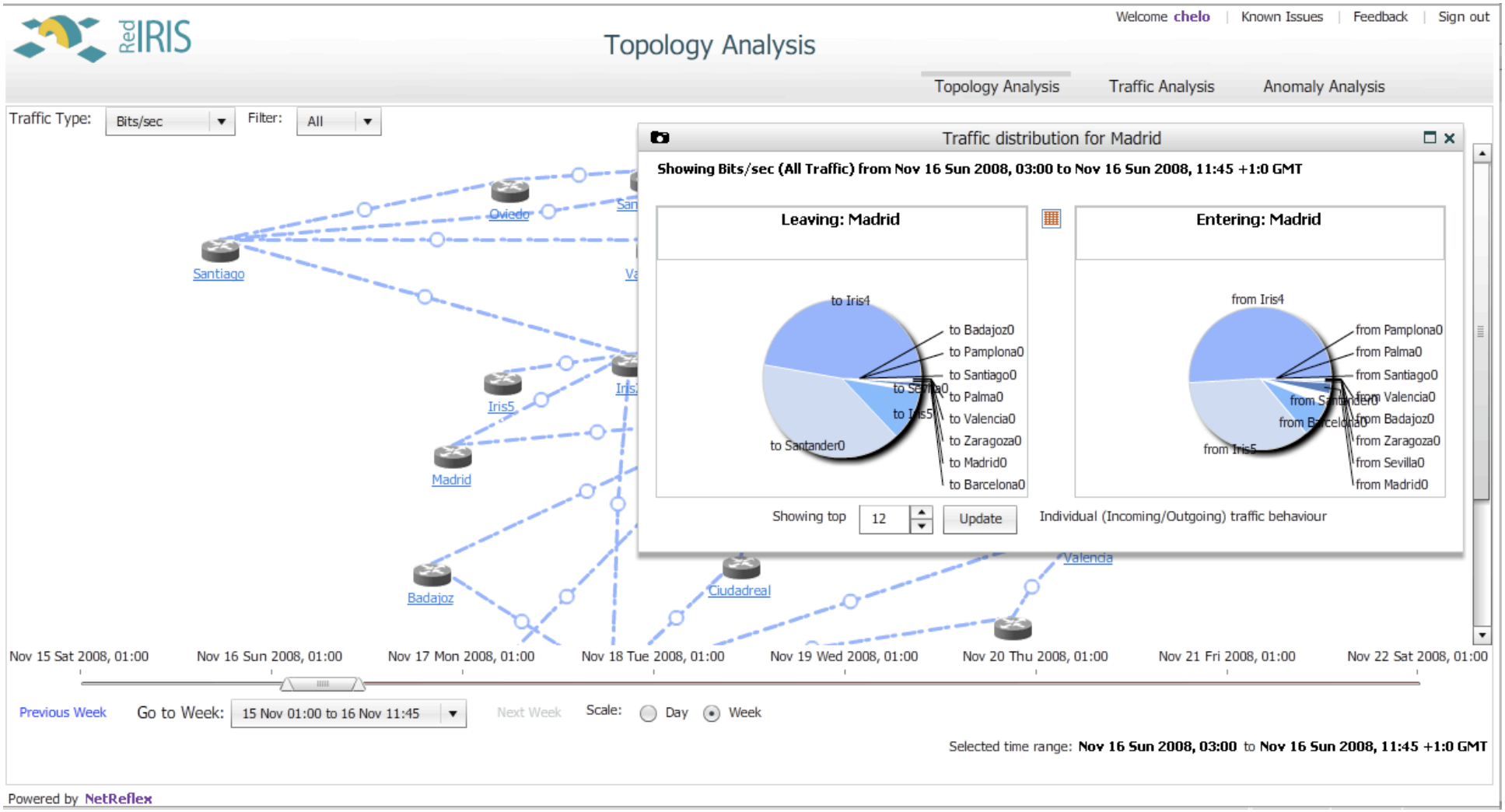
Nuevas Iniciativas

Pruebas detección anomalías - NetReflex

- Apliance (comercial) para la detección y diagnosis de anomalías de red (ataques y anomalías de routing), a partir de datos NetFlow y de routing (BGP e ISIS/OSPF)
  - Proyecto de investigación de la Universidad de Boston (Intel/ SpringLabs) ➔ Gauvus Inc
  - Network-wide Data Mining
    - El tráfico total de la red se particiona en pequeños subconjuntos. Sobre ellos se determinar qué es normal y qué no, correlándolos
- JRA2 ("Security") de GN2
  - Detección de anomalías avanzada ➔ Ampliación Toolset
- (beta testers) Dante + RedIRIS
  - Detección automática, clasificación e identificación espacial de anomalías de seguridad
  - Elaboración de tablas comparativas entre herramientas similares
  - Soporte para la creación de Dante CERT

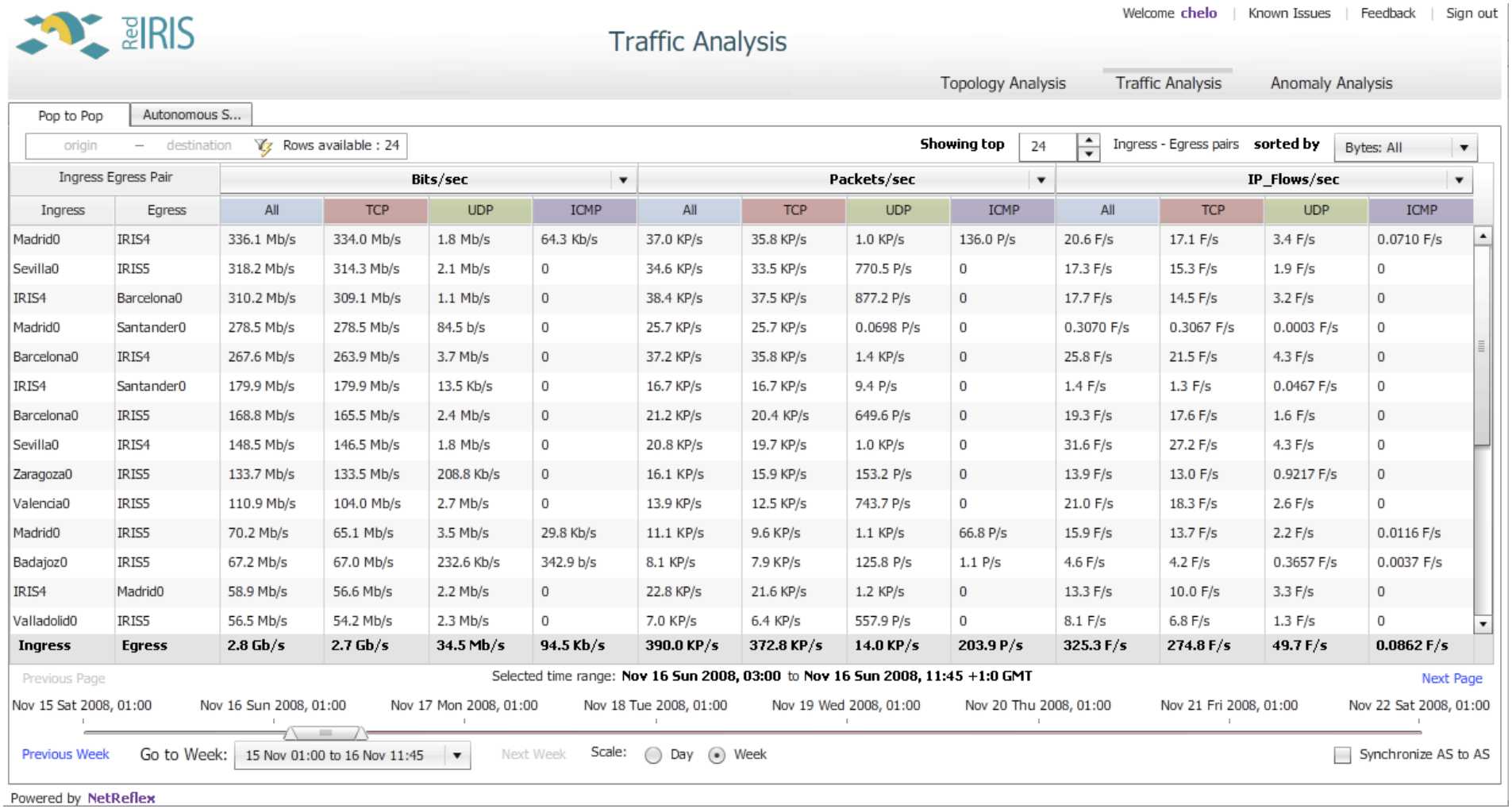
NetReflex – Vistas (I)

- Análisis de la topología de red



NetReflex – Vistas (II)

- Análisis de tráfico



Red IRIS

Welcome chelo | Known Issues | Feedback | Sign out

Traffic Analysis

Topology Analysis | Traffic Analysis | Anomaly Analysis

Pop to Pop | Autonomous S...

origin – destination | Rows available : 24

Showing top 24 Ingress - Egress pairs sorted by Bytes: All

Ingress Egress Pair		Bits/sec				Packets/sec				IP_Flows/sec			
Ingress	Egress	All	TCP	UDP	ICMP	All	TCP	UDP	ICMP	All	TCP	UDP	ICMP
Madrid0	IRIS4	336.1 Mb/s	334.0 Mb/s	1.8 Mb/s	64.3 Kb/s	37.0 KP/s	35.8 KP/s	1.0 KP/s	136.0 P/s	20.6 F/s	17.1 F/s	3.4 F/s	0.0710 F/s
Sevilla0	IRIS5	318.2 Mb/s	314.3 Mb/s	2.1 Mb/s	0	34.6 KP/s	33.5 KP/s	770.5 P/s	0	17.3 F/s	15.3 F/s	1.9 F/s	0
IRIS4	Barcelona0	310.2 Mb/s	309.1 Mb/s	1.1 Mb/s	0	38.4 KP/s	37.5 KP/s	877.2 P/s	0	17.7 F/s	14.5 F/s	3.2 F/s	0
Madrid0	Santander0	278.5 Mb/s	278.5 Mb/s	84.5 b/s	0	25.7 KP/s	25.7 KP/s	0.0698 P/s	0	0.3070 F/s	0.3067 F/s	0.0003 F/s	0
Barcelona0	IRIS4	267.6 Mb/s	263.9 Mb/s	3.7 Mb/s	0	37.2 KP/s	35.8 KP/s	1.4 KP/s	0	25.8 F/s	21.5 F/s	4.3 F/s	0
IRIS4	Santander0	179.9 Mb/s	179.9 Mb/s	13.5 Kb/s	0	16.7 KP/s	16.7 KP/s	9.4 P/s	0	1.4 F/s	1.3 F/s	0.0467 F/s	0
Barcelona0	IRIS5	168.8 Mb/s	165.5 Mb/s	2.4 Mb/s	0	21.2 KP/s	20.4 KP/s	649.6 P/s	0	19.3 F/s	17.6 F/s	1.6 F/s	0
Sevilla0	IRIS4	148.5 Mb/s	146.5 Mb/s	1.8 Mb/s	0	20.8 KP/s	19.7 KP/s	1.0 KP/s	0	31.6 F/s	27.2 F/s	4.3 F/s	0
Zaragoza0	IRIS5	133.7 Mb/s	133.5 Mb/s	208.8 Kb/s	0	16.1 KP/s	15.9 KP/s	153.2 P/s	0	13.9 F/s	13.0 F/s	0.9217 F/s	0
Valencia0	IRIS5	110.9 Mb/s	104.0 Mb/s	2.7 Mb/s	0	13.9 KP/s	12.5 KP/s	743.7 P/s	0	21.0 F/s	18.3 F/s	2.6 F/s	0
Madrid0	IRIS5	70.2 Mb/s	65.1 Mb/s	3.5 Mb/s	29.8 Kb/s	11.1 KP/s	9.6 KP/s	1.1 KP/s	66.8 P/s	15.9 F/s	13.7 F/s	2.2 F/s	0.0116 F/s
Badajoz0	IRIS5	67.2 Mb/s	67.0 Mb/s	232.6 Kb/s	342.9 b/s	8.1 KP/s	7.9 KP/s	125.8 P/s	1.1 P/s	4.6 F/s	4.2 F/s	0.3657 F/s	0.0037 F/s
IRIS4	Madrid0	58.9 Mb/s	56.6 Mb/s	2.2 Mb/s	0	22.8 KP/s	21.6 KP/s	1.2 KP/s	0	13.3 F/s	10.0 F/s	3.3 F/s	0
Valladolid0	IRIS5	56.5 Mb/s	54.2 Mb/s	2.3 Mb/s	0	7.0 KP/s	6.4 KP/s	557.9 P/s	0	8.1 F/s	6.8 F/s	1.3 F/s	0
Ingress	**Egress**	**2.8 Gb/s**	**2.7 Gb/s**	**34.5 Mb/s**	**94.5 Kb/s**	**390.0 KP/s**	**372.8 KP/s**	**14.0 KP/s**	**203.9 P/s**	**325.3 F/s**	**274.8 F/s**	**49.7 F/s**	**0.0862 F/s**

Previous Page | Selected time range: **Nov 16 Sun 2008, 03:00** to **Nov 16 Sun 2008, 11:45 +1:0 GMT** | Next Page

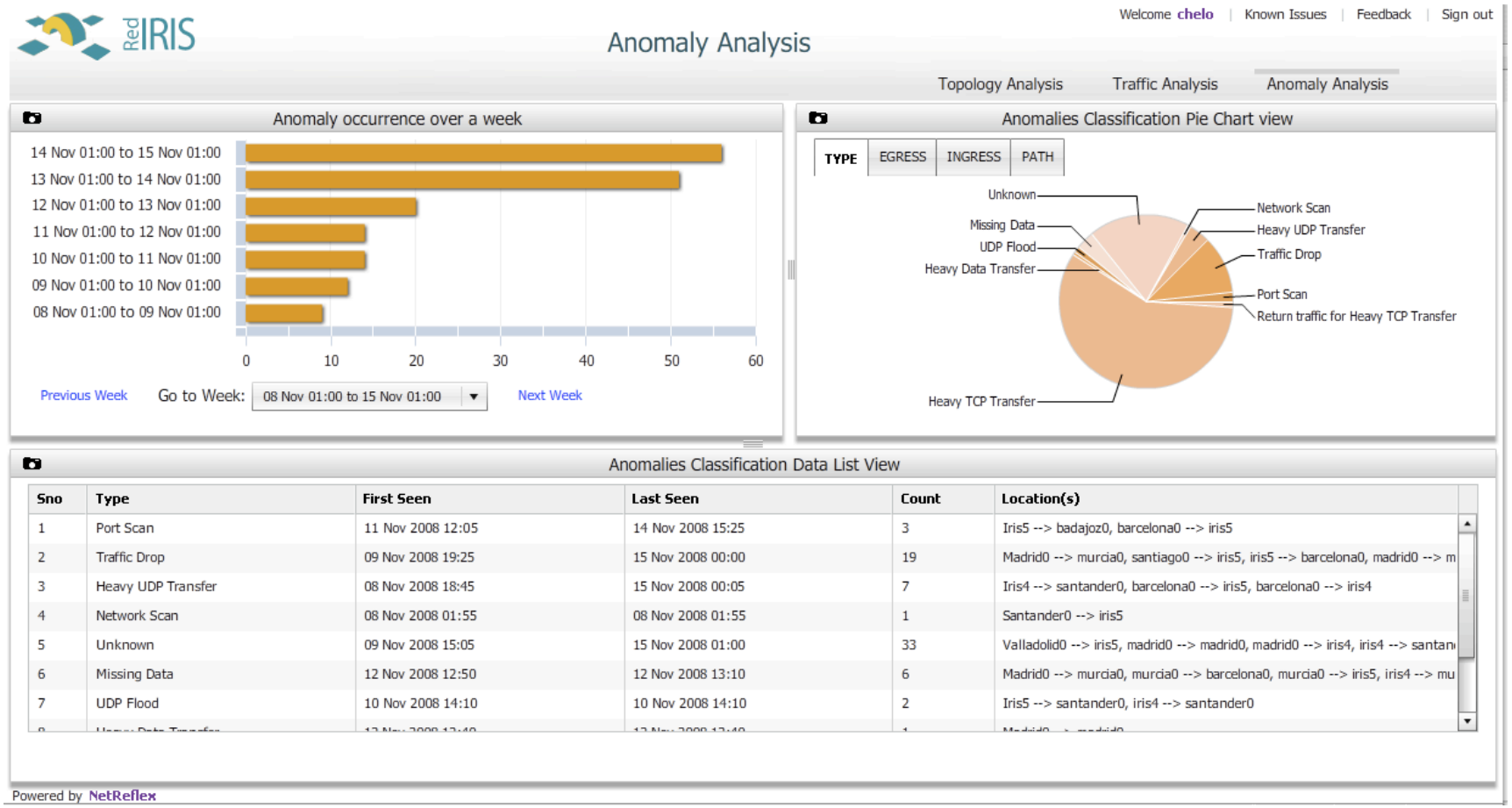
Nov 15 Sat 2008, 01:00 | Nov 16 Sun 2008, 01:00 | Nov 17 Mon 2008, 01:00 | Nov 18 Tue 2008, 01:00 | Nov 19 Wed 2008, 01:00 | Nov 20 Thu 2008, 01:00 | Nov 21 Fri 2008, 01:00 | Nov 22 Sat 2008, 01:00

Previous Week | Go to Week: 15 Nov 01:00 to 16 Nov 11:45 | Next Week | Scale: Day Week | Synchronize AS to AS

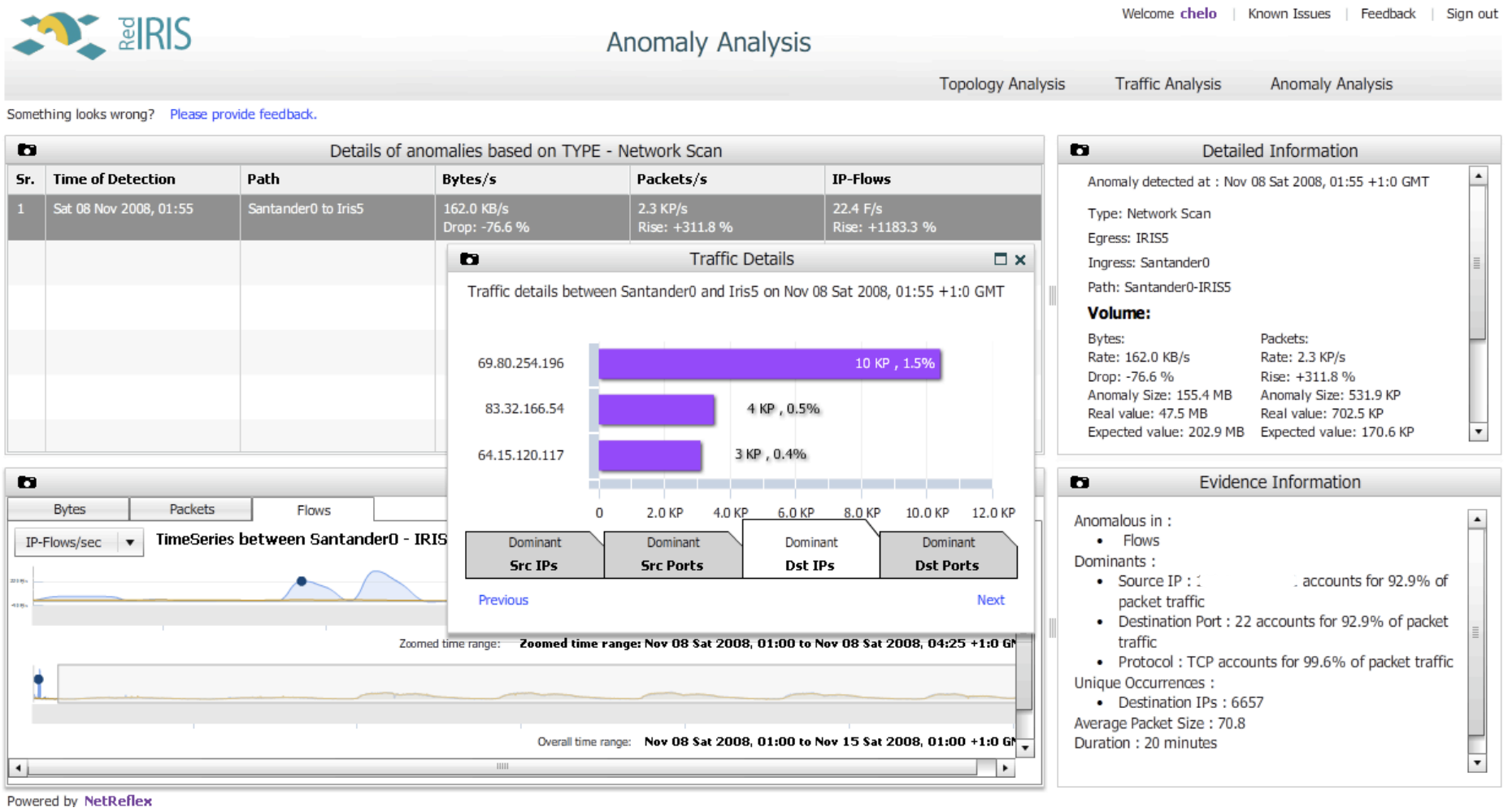
Powered by NetReflex

NetReflex – Vistas (III)

- Análisis de anomalías
  - Detección, localización y clasificación
  - DoS/DDoS, (distributed) port y network scan, (distributed) spam



Análisis de anomalías



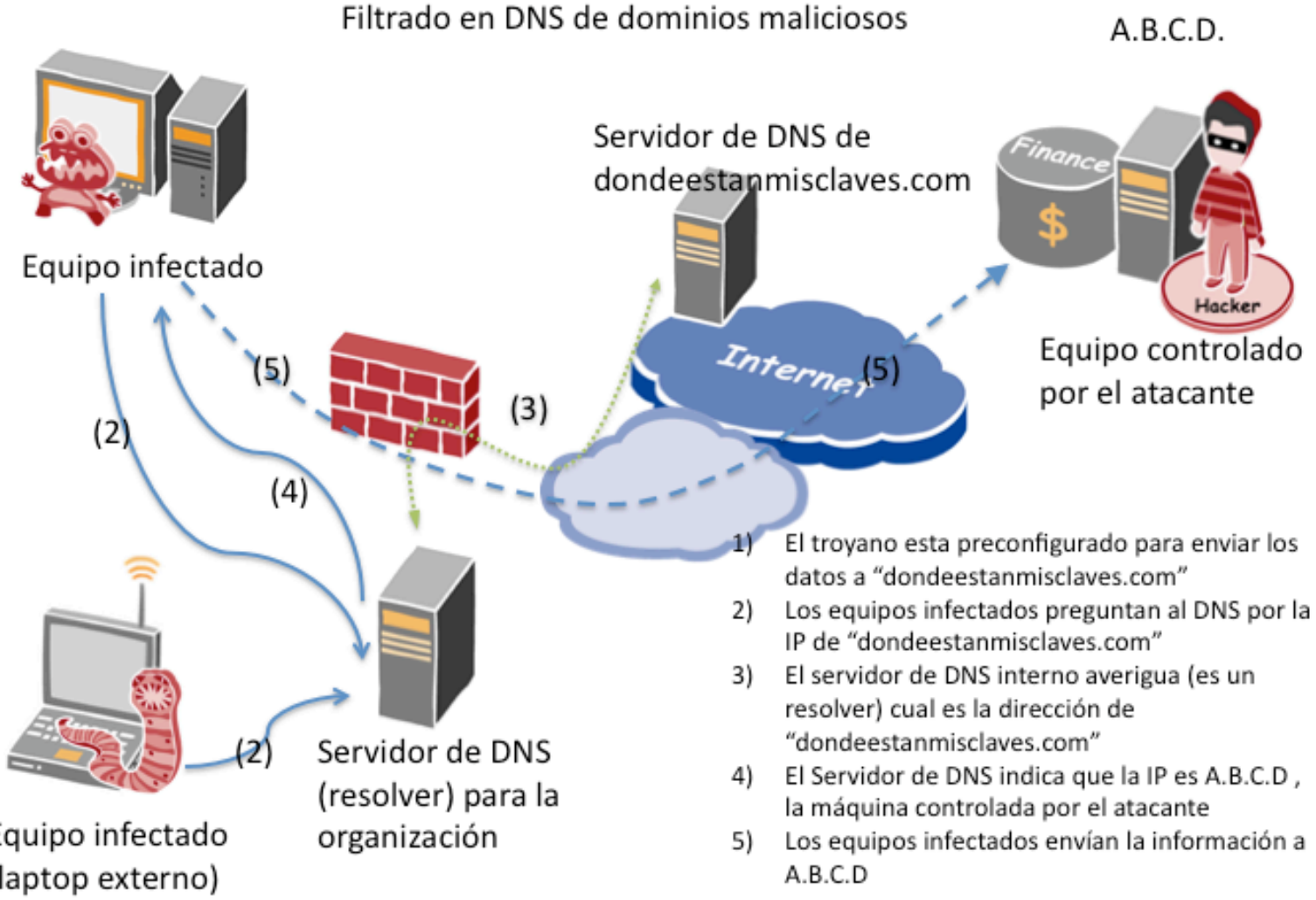
- Fin de pruebas Enero 2009
  - En espera conclusiones Grupo JRA2 ➔ DJ2.2.4,2
  - Oferta económica no competitiva
  - Buenos resultados en la detección automática, clasificación y identificación espacial de anomalías
  - Herramienta poco madura
    - ➢ En estos momentos no es 100% útil para el trabajo diario de un CERT
      - ❖ Análisis forense, utilidades de búsqueda, programación de eventos, alertas (notificación automática ..), informes, API Programable, correlación …
  - Falta comparación con otras herramientas similares (Stager, Qradar, StealthWatch, …)
    - ➢ Complementarias a los sistemas tradicionales de detección
  - Ayudadnos a localizar falsos positivos

DNS blackholeing (I)

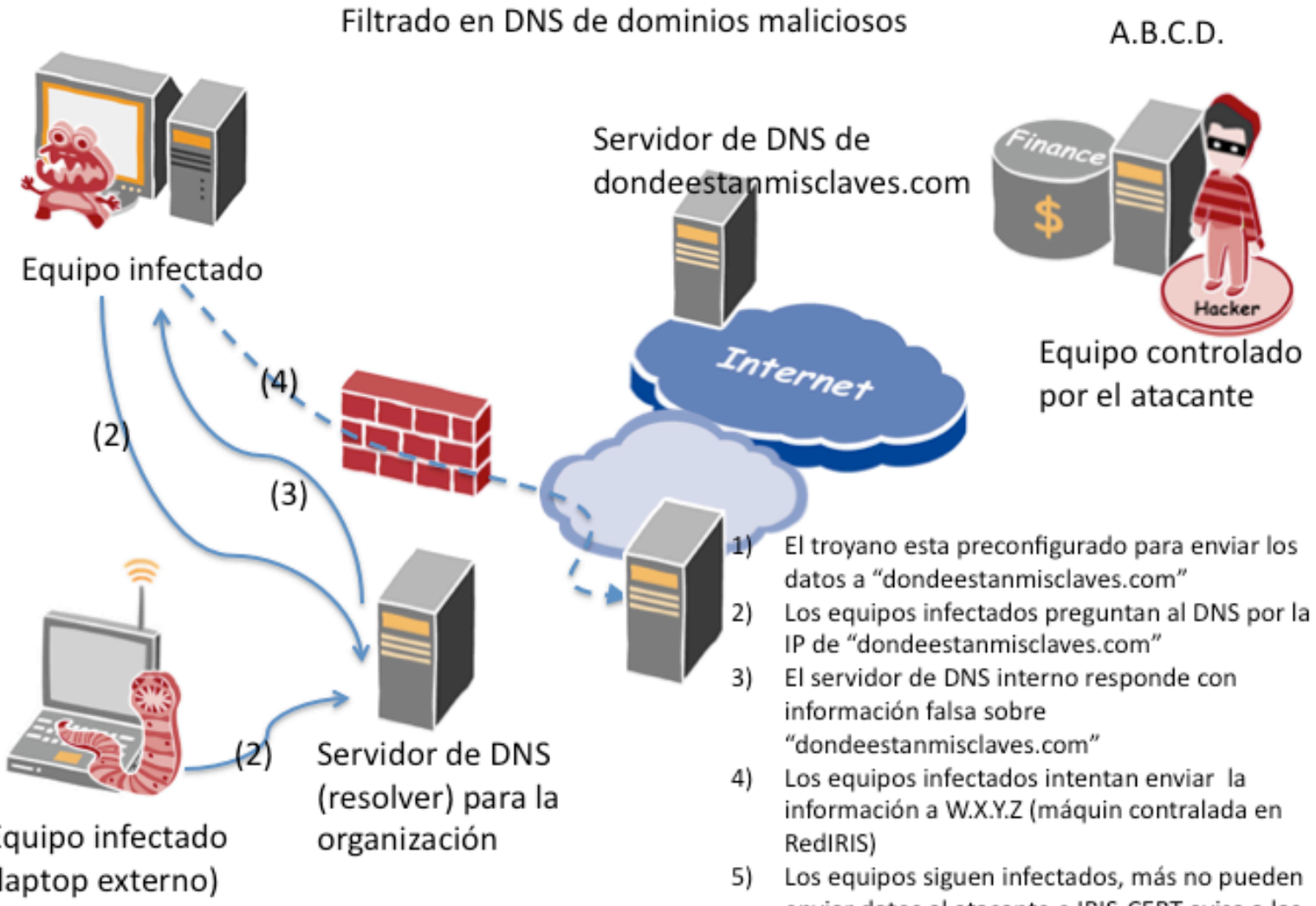
- Mecanismo de bloqueo en el DNS de dominios empleados por programas maliciosos
  - Se pueden bloquear dominios de Keyloggers, IRC, fast-flux, redirecciones de iframes en web infectadas
  - ≅ 729 dominios monitorizados
  - Fuentes privadas, de incidentes, otros CERTs, …
- Monitorización de peticiones Web
  - Detección de máquinas comprometidas y páginas infectadas

http://www.rediris.es/cert/proyectos/dns-black/

Funcionamiento de un keylogger

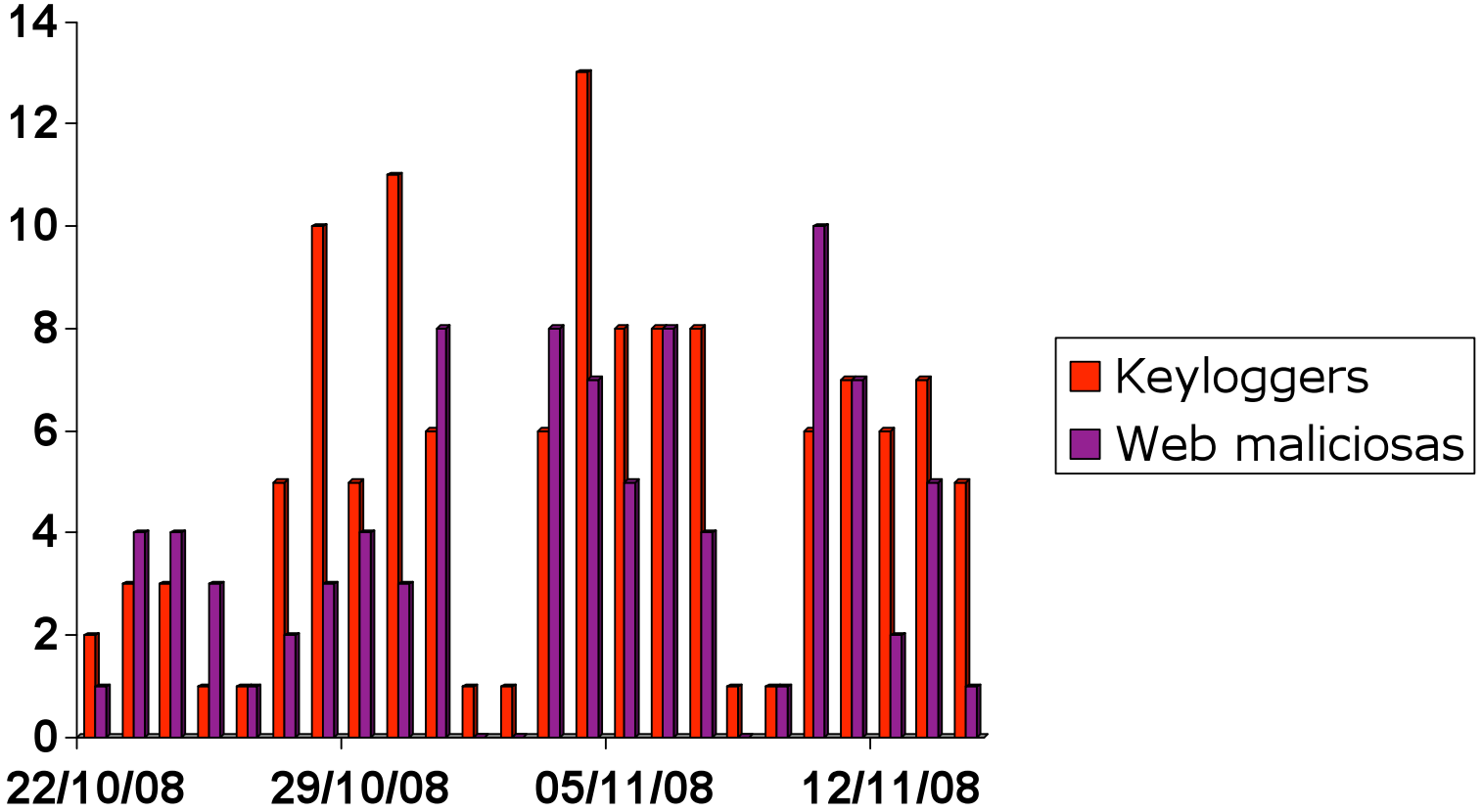


DNS configurado como "master" de dominios maliciosos



Estado actual

- 15 instituciones utilizan el sistema en pruebas
- Trabajo futuro
  - Notificación automática, integración RTIR, inclusión de más dominios maliciosos, HTTP para incluir/eliminar nuevos dominios en el named.conf, colaborar con iniciativas similares



Cursos y Eventos

- Foro de Seguridad
  - Segunda o tercera semana de Marzo 2009
  - Monográfico día y medio
  - ¿Temas?
    - Arquitecturas seguras
    - Temas legales
    - Técnicas de detección/prevención ataques
    - Análisis Forense
    - …. Vosotros decidís!!!

- Curso teórico/práctico nfsen (GN2)
  - Madrid, 15 Enero 2009
  - 15-20 personas
  - Prácticas sobre un entorno nfsen simulado (VMWare)
    - Preguntas/respuestas sobre datos netflow reales (anonimizados/ISP mediano)

- Otra opción …
  - Zurich, 2-4 Febrero 2009
  - + TERENA Train Trainers + GN2 Toolset completo

THE END .....

Red
Académica y de Investigación
Española

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