Contenido

- Motivación
- Esquema general
  - Fuentes de información
  - Formatos aceptados
- Diseño
  - Base de datos
  - Filtrado de direcciones IP
  - Filtrado de flujos
  - Formato de las direcciones
  - Script de descarga
- Resultados
- Conclusiones y trabajo futuro

Motivación

- Botnet: conjunto de ordenadores “zombies” conectados a internet, que interactúan para realizar alguna tarea distribuida de objetivo ilegal.
- Son un problema para los administradores de red
  - Son fuentes de SPAM y ataques a otras redes
- Es necesario establecer mecanismos que permitan estimar la incidencias en la red administrada.
- Fuentes de información disponibles: listas negras
  - Aplicación sobre rangos de direcciones IP y sobre registros de Netflow

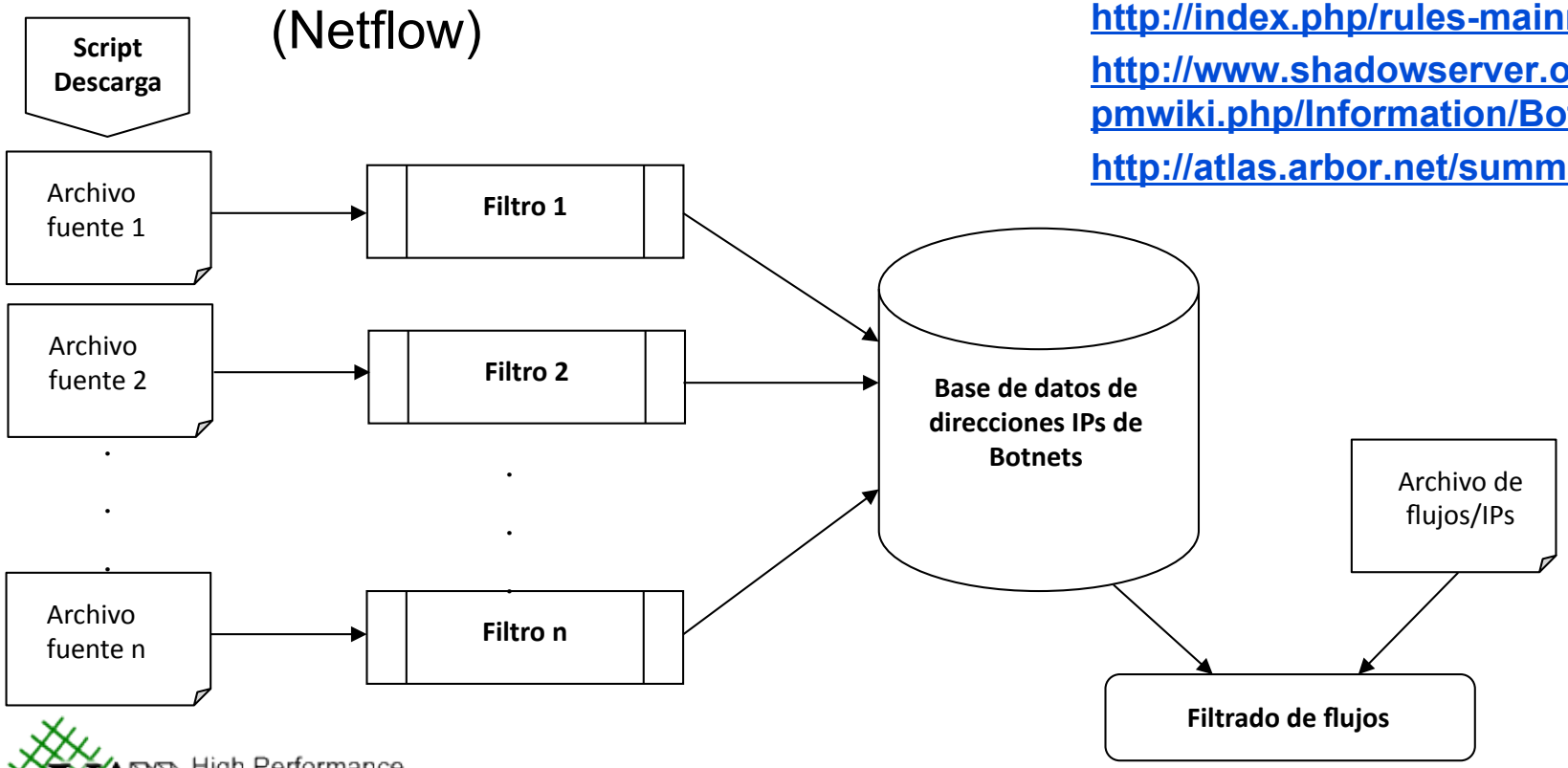
Esquema general

Formatos aceptados

- Listado de direcciones con formato IP/máscara
- Fichero con flujos de red (Netflow)

Fuentes de información

http://www.dshield.org/
http://www.trustedsource.org/
http://www.spamcop.net/
http://isc.sans.org/ipinfo.html
http://index.php/rules-mainmenu-38.html
http://www.shadowserver.org/wiki/pmwiki.php/Information/Botnets
http://atlas.arbor.net/summary/botnets



Diseño

Base de datos

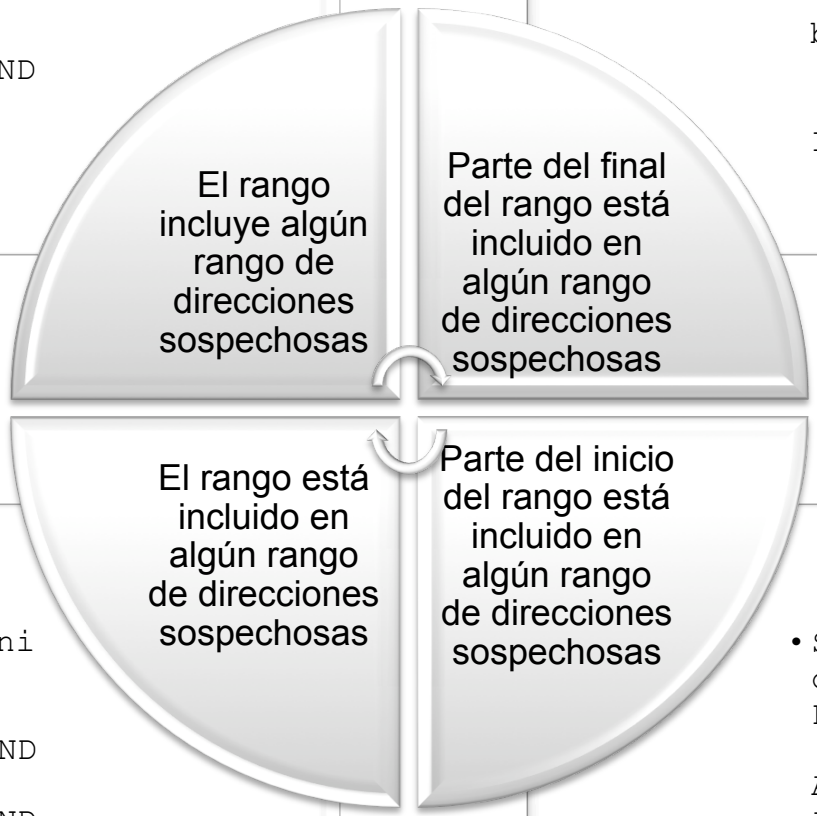
- Tabla de direcciones IP obtenidas de las listas negras:
  - IP inicial
  - IP final
  - Tipo
    - Botnet
    - Spam
    - Ataque: No especifican el tipo o son distintas de spam o botnet
  - Fecha de inicio
  - Fecha fin
- Tamaño de la BD muy grande
  - Se tarda mucho en realizar las consultas de búsqueda de IPs
  - Indexación usando un árbol B sobre IP inicial e IP final
    - Permite operaciones >, <, >=, <= además del = permitido en Hash

Diseño

Filtrado de rangos de direcciones IP

- SELECT (IPfinal- IPfinal +1) AS num, tipo FROM baseDatosBot WHERE (IPinicial > direIni) AND (IPfinal < direFin)

- SELECT (direFin-IPinicial +1) AS num, tipo FROM baseDatosBot WHERE (IPinicial > direIni) AND (IPinicial <= direFin AND IPfinal >= direFin)



- SELECT (direFin – direIni +1) AS num, tipo FROM baseDatosBot WHERE (IPinicial <= direIni AND IPfinal >= direIni) AND (IPinicial <= direFin AND IPfinal >= direFin)

- SELECT (IPfinal - direIni+1) AS num, tipo FROM baseDatosBot WHERE (IPinicial <= direIni AND IPfinal >=direIni) AND (IPfinal< direFin)

Diseño

Filtrado de flujos de red (NetFlow)

```
SELECT *
FROM baseDatosBot
WHERE  (IPinicial <= direccionIni AND IPfinal>= direccionIni)
OR (IPinicial <=direccionFin AND IPfinal>= direccionFin)
```

Formato de las direcciones IP

- Conversión de formato IP a entero de 32 bits
  - Comparaciones menos costosas.

Script de descarga

- Se basa en el uso de wget para la descarga de archivos desde servidores web.
- Realiza la llamada a la aplicación automáticamente para la actualización de la fecha y el filtrado de los ficheros

Resultados

- Todas las pruebas presentadas se basan en un base de datos con direcciones IP recogidas el día 14/09/2010.
- Los flujos de RedIRIS utilizados también se corresponden con dicha fecha.
- Los Netflows usados en las pruebas tienen un muestreo de 1:1000.

Resultados

- Rangos de direcciones IP
  - De un nodo de RedIRIS
  - De un conjunto de 10 universidades dispersas geográficamente
  - Del conjunto de RedIRIS
- Registros de Netflow
  - De un nodo de Rediris
  - De un conjunto de 10 universidades dispersas geográficamente
  - **Para el conjunto RedIRIS no sería viable en un tiempo razonable, salvo usando muchos equipos en paralelo**

Resultados

Rango de direcciones IP de un nodo de RedIris

BD	# direcciones nodo RedIris				Tiempo (ms)		
# IPs	Botnets	Spam	Otros	Total	Total	Filtrado	Estimación
14801	**2**	**0**	**0**	**87032**	**850**	**63**	**787**

- Las direcciones (anonimizadas) de las dos botnets que se han detectado se visualizan del siguiente modo en el fichero de salida:

```
x.147.162.98 botnet
y.214.188.23 botnet
```

Resultados

Rango de direcciones IP de 10 universidades

- Sólo afectada una IP de una universidad
  - `z.88.229.16 botnet`

Rango de direcciones IP de RedIRIS (18 nodos)

- Nodo x
  - `x1.156.51.124 botnet`
  - `x2.156.252.198 botnet`
- Nodo y
  - `y1.214.188.23 botnet`
  - `y2.147.162.98 botnet`
- Nodo z
  - `z1.88.229.16 botnet`
  - `z2.128.144.98 botnet`

⇨ Son pocas pero hay que tener en cuenta que en las listas negras sólo se almacenan las direcciones de command&control

Resultados

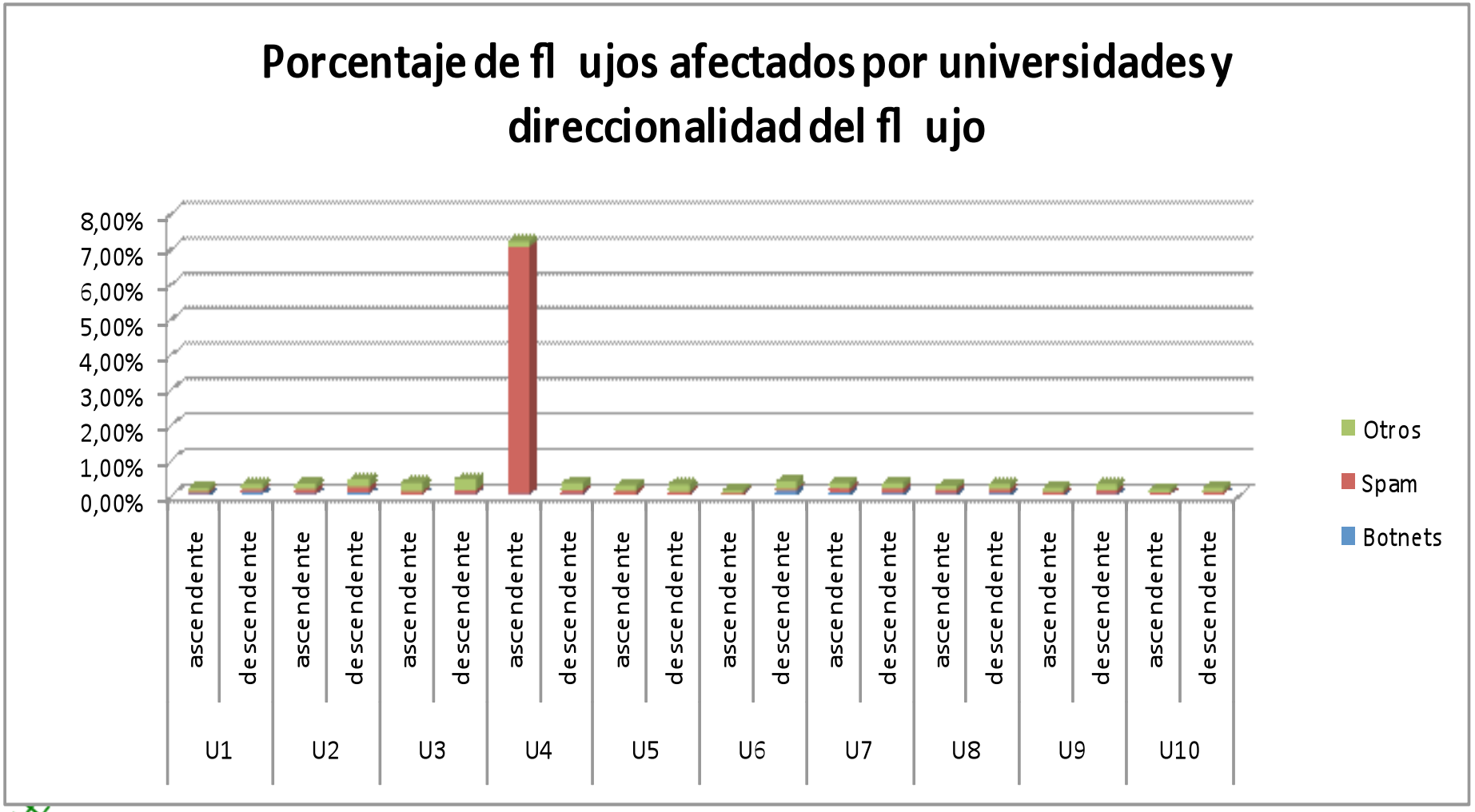
Registros de Netflow de un nodo de RedIris

BD	# flujos nodo RedIris				Tiempo
# IPs	Botnets	Spam	Otros	Total	(ms)
14801	**654945**	**34279**	**30039**	**24994108**	**73312960**

- A pesar de que anteriormente sólo se habían detectado dos direcciones de botnet, se puede ver que hay un número de flujos significativo con direcciones que se encuentran en listas negras.

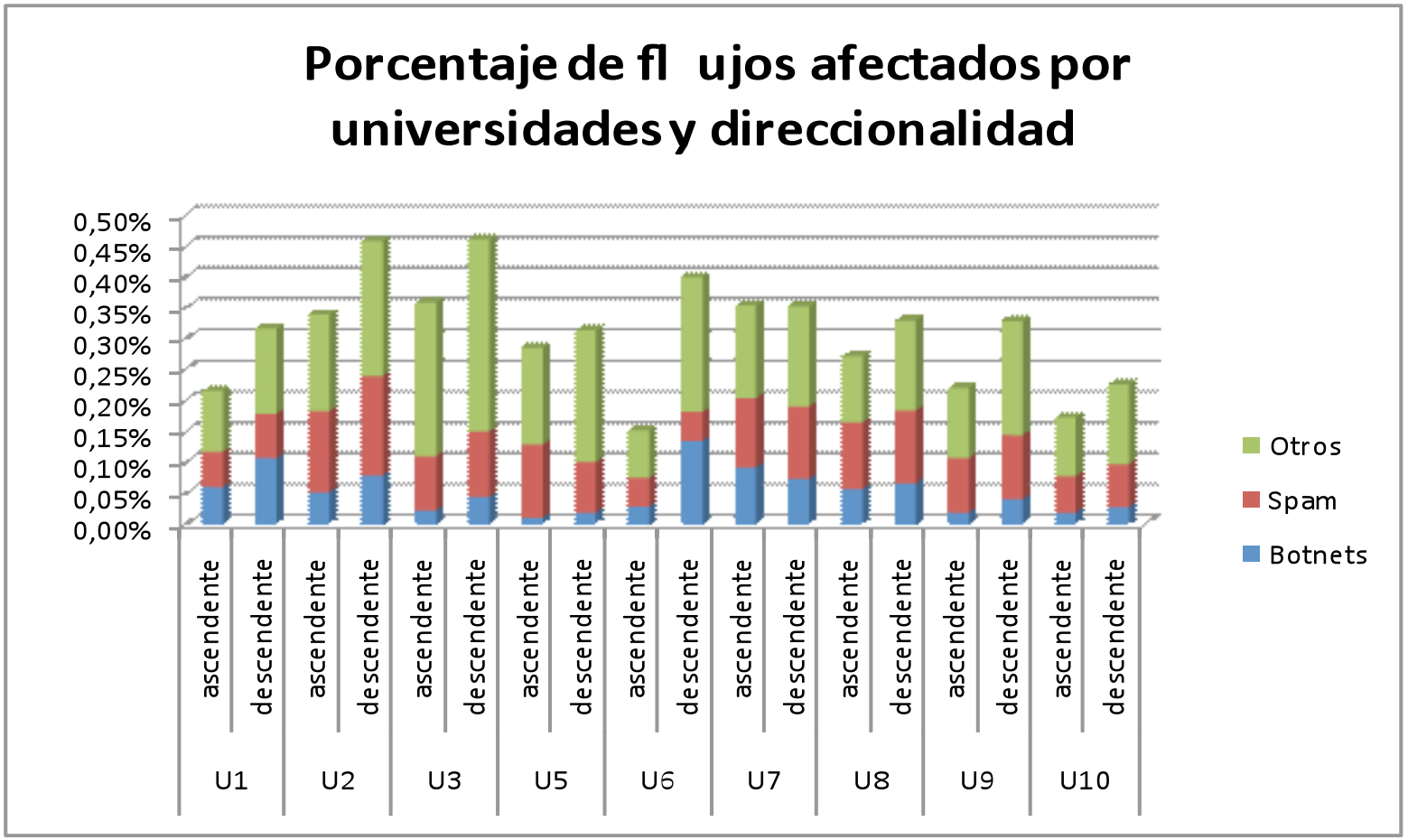
Resultados

Registros de Netflow para 10 universidades



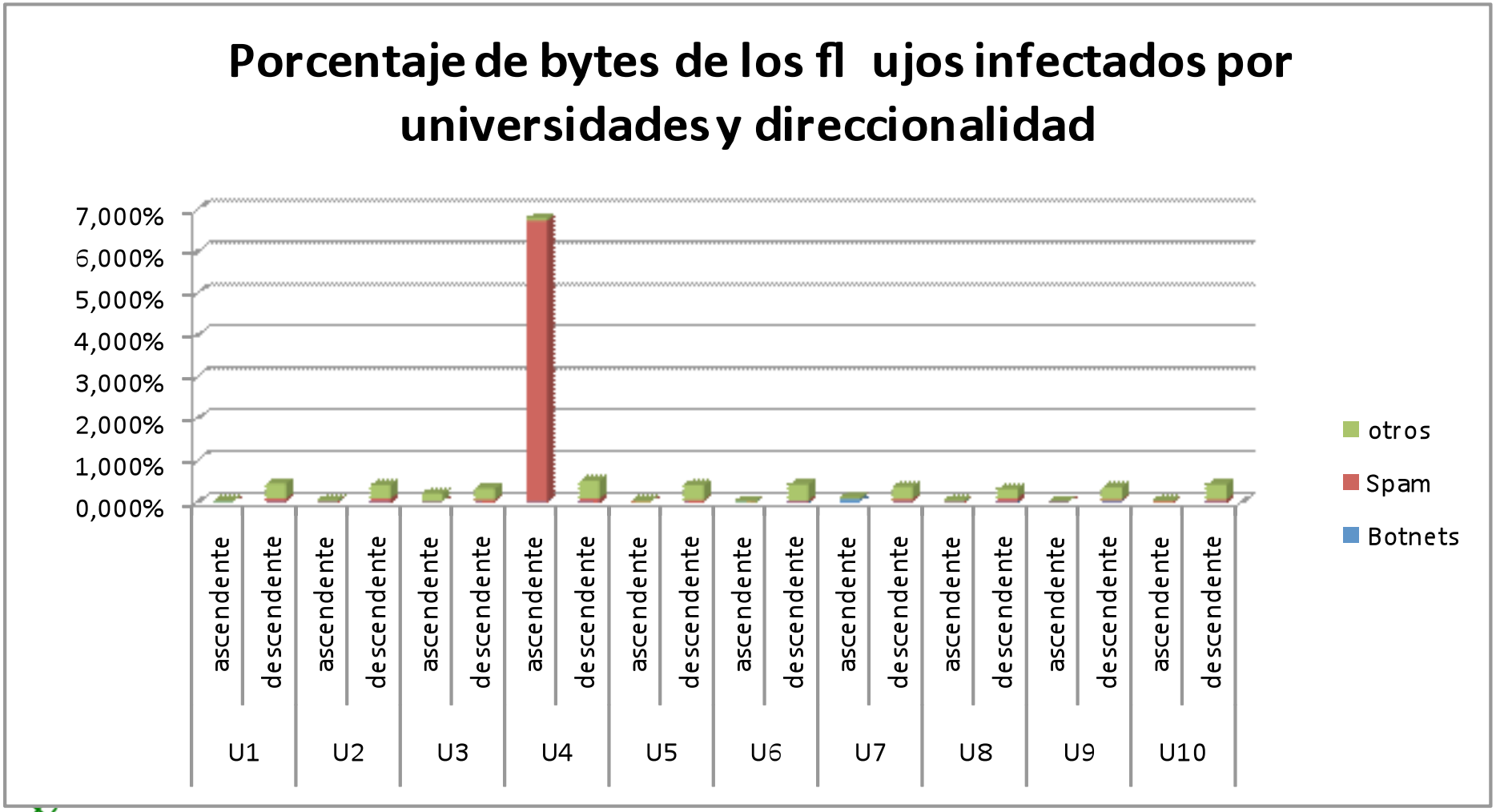
Resultados

Registros de Netflow para 10 universidades



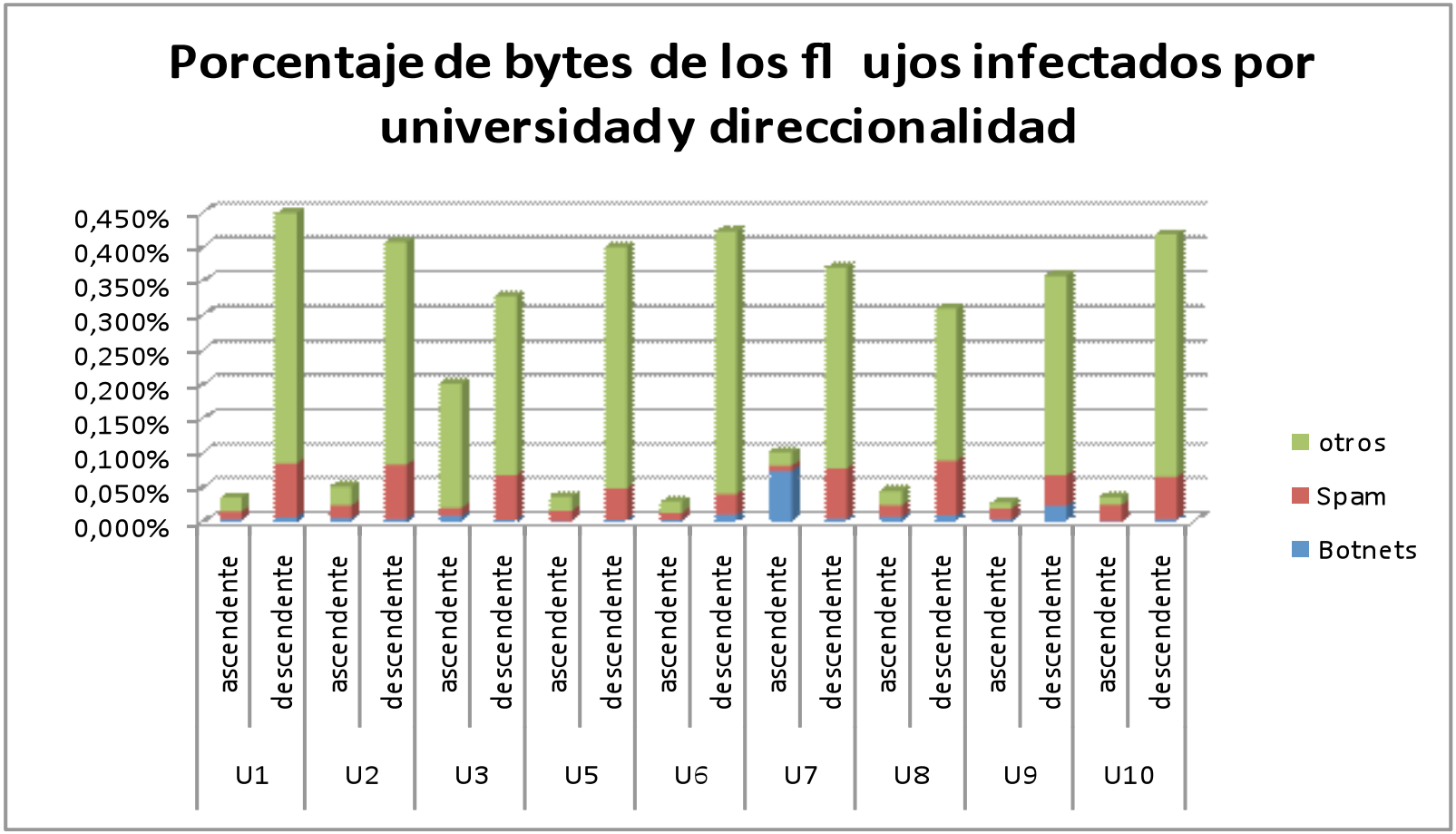
Resultados

Registros de Netflow para 10 universidades



Resultados

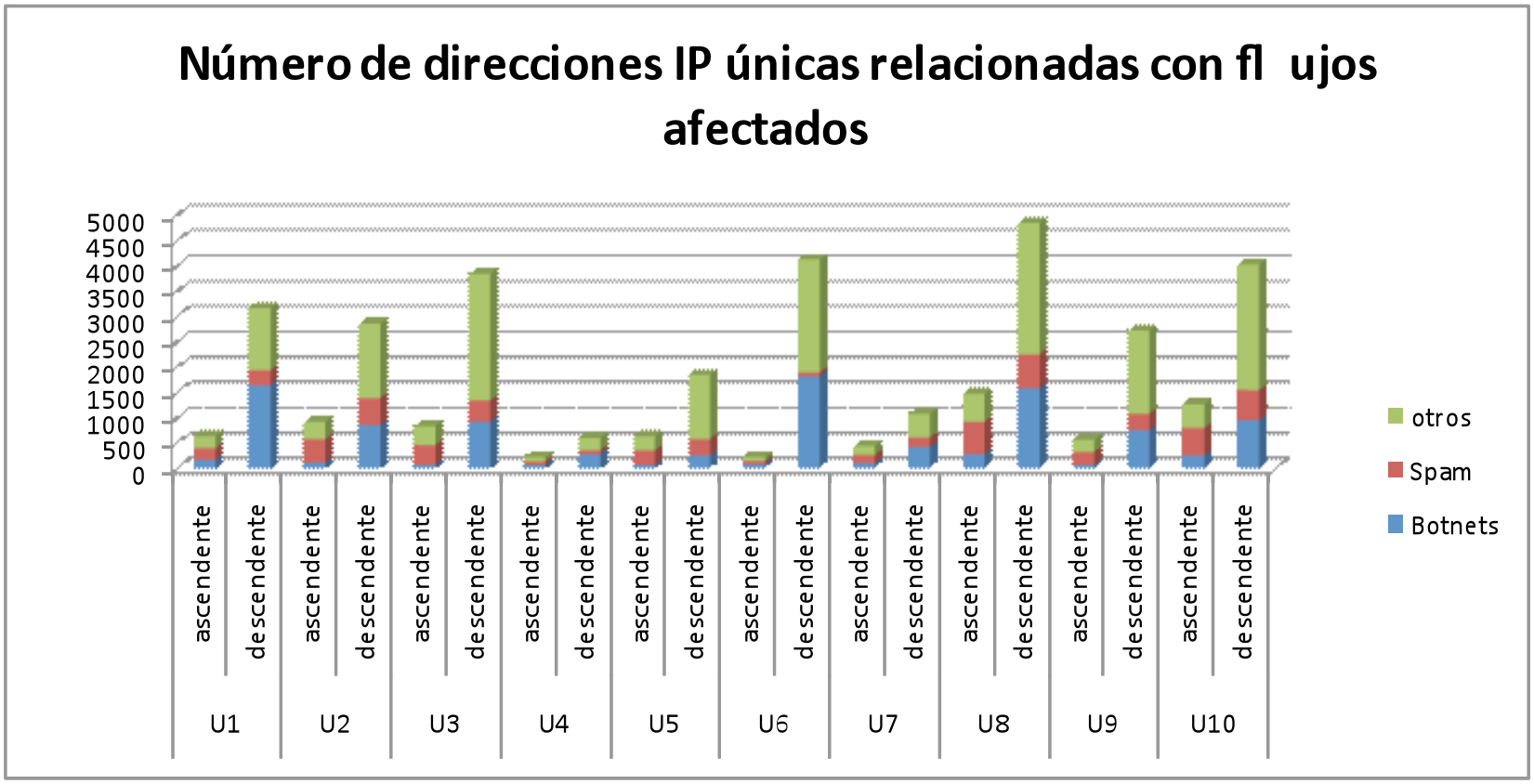
Registros de Netflow para 10 universidades



Resultados

Registros de Netflow para 10 universidades

⇨ También es importante saber cuántas y cuáles direcciones de RedIRIS están teniendo contacto con direcciones incluidas en listas negras



Conclusiones

- Aunque parezca que hay poca incidencia, las botnets pueden despertar.
- Se detectan más flujos descendentes que ascendentes.
- Es interesante ver la relación entre flujos ascendentes y descendentes
  - Problema→ Muestreo de flujos.
- Los tiempos de ejecución no son muy altos pero es clave para el análisis en el tiempo de la variación de botnets
- Limitación → el uso solo de listas negras
  - No detección de botnets no identificadas en las listas
  - Tendencia peer-to-peer de las botnets

Trabajos futuros

- Afinar la incidencia de botnets
  - A partir de la existencia de flujos ascendente y descendente
  - A partir del número de bytes y paquetes de cada flujo detectado
- Mejora del rendimiento
  - Procesos concurrentes