Monitoreo y Protección de Infraestructura Crítica

GRUPO TELECOM

SOC Seguridad Informática – Telecom Argentina S.A.

MAYO 2014

Introducción

Objetivos

- **Sintetizar nuestro contexto como prestador *Tier-2* de acceso a Internet y proveedor de servicios de comunicaciones.**
- **Transmitir, desde nuestra experiencia basada en eventos reales y lecciones aprendidas, algunos de los conceptos bajo los cuales procuramos maximizar el nivel de servicio de nuestros elementos de red.**
- **Compartir algunos criterios de monitoreo y control que aplicamos diariamente.**
- **Exponer nuestra experiencia en la problemática de los ataques distribuidos y el hacktivismo.**

Agenda

- Telecom Argentina como Operador *Tier-2*
  - Oferta de Servicios
  - Nuestros Datacenters
  - Nuestro Backbone IP
  - Contexto y Riesgos
- Nuestro SOC
- Criterios de Monitoreo y Control
  - Configuración de Nodos de Red
  - Gestión de Infraestructura
  - Detección de Actividad Inusual
- Ataques contra Recursos de Misión Crítica
  - "DDoS" - Definición
  - Aspectos Técnicos y Contexto
  - El Enfoque de Telecom Argentina
  - Magnitudes y Tendencias
- Hacktivismo
  - Casos Recientes de Público Conocimiento
  - Nuestros Recursos como Objetivo de Ataque

Telecom Argentina como Operador *Tier-2 (cont.)*

Oferta

- Telefonía fija.
- Telefonía móvil.
- Banda ancha.
- Enlaces de datos de alta velocidad.
- Transmisión de audio y video.
- Hosting y housing en datacenters.
- Servicios Cloud.
- *(entre otros)*

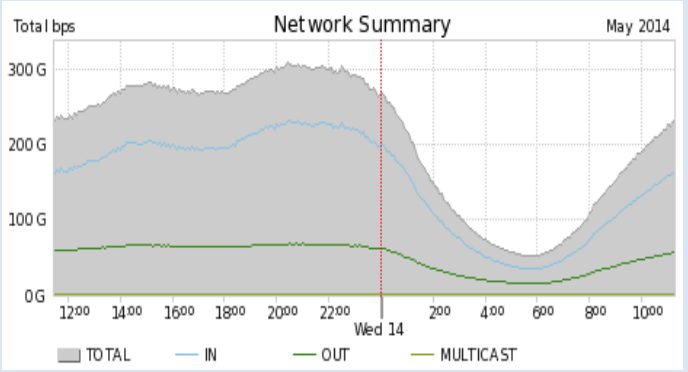
Nuestros DataCenters

- 4 Datacenters distribuidos geográficamente.
- Tier-3.
- Certificaciones:
  - SAS-70 tipo II.
  - A4609 BCRA.
  - ISO 27001 Seguridad de la Información del SOC.
  - ISO 9001 Procesos del SOC.
  - ISO 9001 Procesos de Grandes Clientes.
  - PCI.
  - SOX Compliant.

Telecom Argentina como Operador *Tier-2*

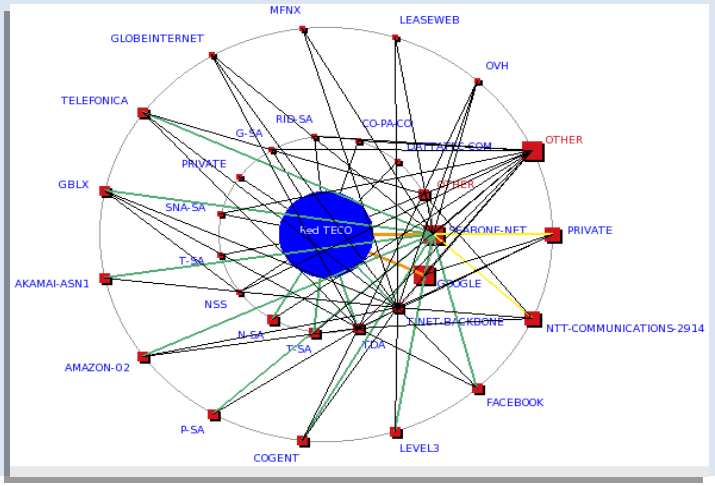
Nuestro BackBone IP

- **Compuesto por más de 21.000 Km de fibra óptica.**
- **Conectado directamente al "anillo" de Tier-1 via NAP de las Américas.**
- **300 Gbps entre tráfico local e internacional.**
- **Aseguramiento y redundancia de todos los caminos.**



Interconexión

- **Contamos con acuerdos de interconexión directa ("peering BGP") con más de 25 entidades entre proveedores y mayoristas lo cual le asegura a nuestros clientes la menor cantidad de "saltos" hacia el contenido de mayor demanda.**



Telecom Argentina como Operador *Tier-2 (cont.)*

Contexto - Riesgos

- **Los riesgos más comunes a los que se ven expuesto Telecom y sus clientes, se encuentran relacionados con los siguientes drivers:**

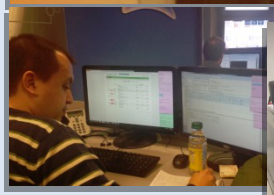
- **Ataques a empresas de telecomunicaciones:**
  - **Las empresas de telecomunicaciones son un blanco preferencial de los hackers ya que además de contar con múltiples puntos de exposición, permiten multiplicar la difusión y alcance de los ataques.**

- **Hacktivismo:**
  - **Las actividades de estos grupos se ven relacionadas con cambios o anuncios de tipo político, social o ambiental.**
  - **Somos proveedores de servicio de organizaciones políticas, organismos regulatorios e instituciones gubernamentales.**

Nuestro SOC

Introducción

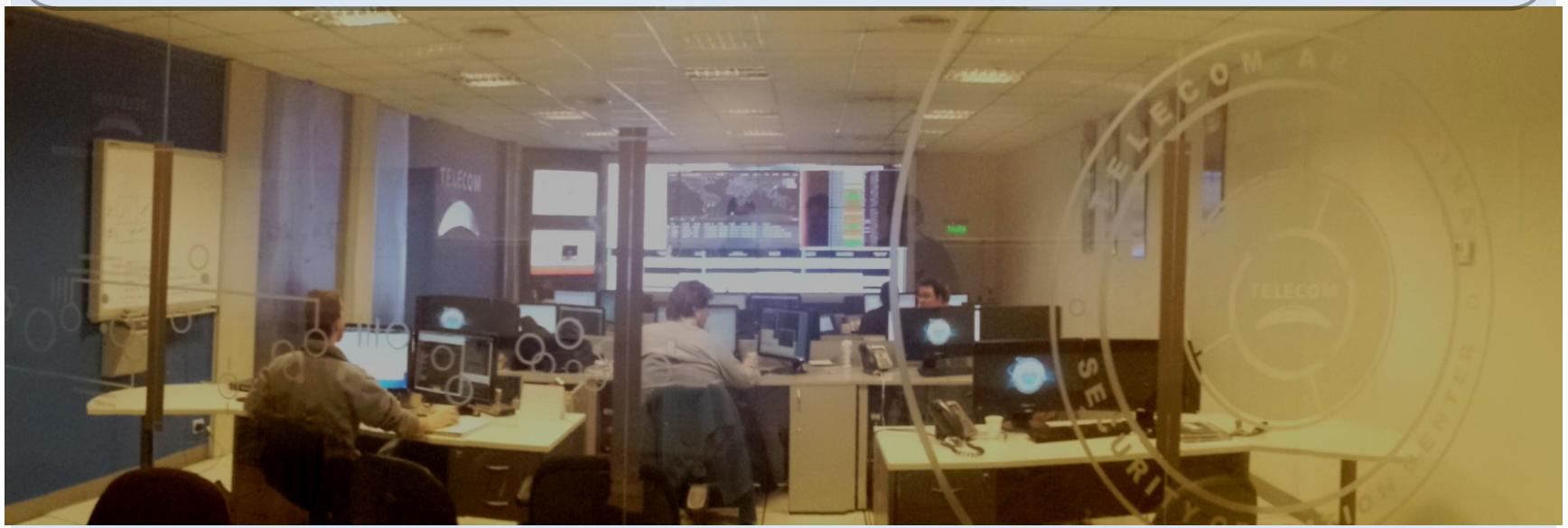
- Nuestro *Centro de Operaciones de Seguridad* que opera las 24 horas de los 365 días del año.
- Su misión consiste en prevenir la ocurrencia de incidentes informáticos de origen externo e interno, detectarlos, y minimizar su impacto en caso de tener lugar.
- Está certificado en ISO/IEC 27001 + ISO 9001 sobre la Gestión Integral de Seguridad de La Información.
- Desde aquí monitoreamos los eventos de seguridad asociados a los sistemas y redes de las empresas del grupo, y de los clientes externos que contratan nuestro servicio.



Nuestro SOC (cont.)

Alcance

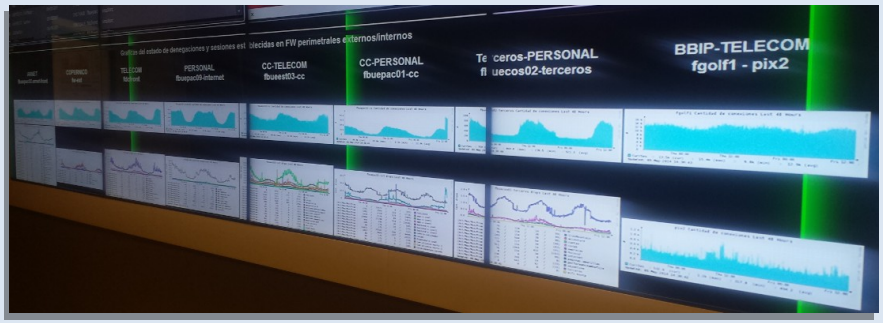
- Perímetro externo (Internet y terceras partes).
- LAN de usuarios a nivel nacional.
- Redes de gestión de infraestructura de misión crítica.
- Datacenters.
- Celdas, centrales e infraestructura de comunicaciones.
- Sistemas de soporte a la operación.
- Nuestro BackBone IP.

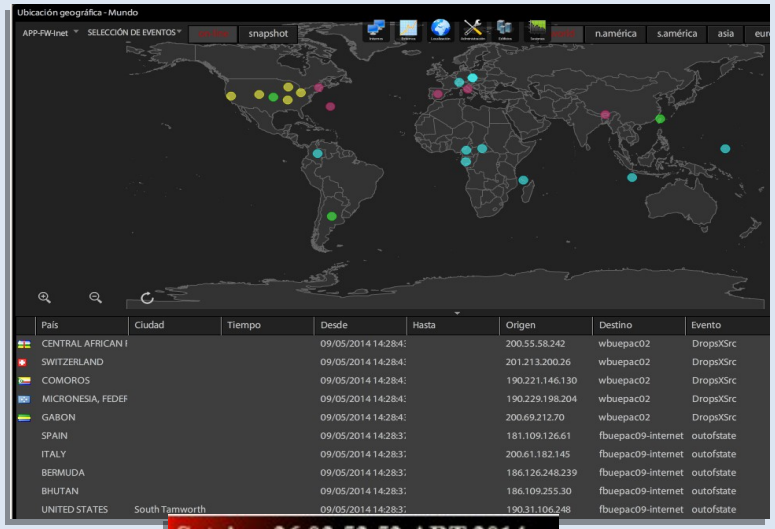


Nuestro SOC (cont.)

Algunos Puntos de Foco de Nuestro Monitoreo Perimetral

- **Geolocalización y bloqueo preventivo de todo origen que presenta:**
  - **Intentos de ataque recurrentes en el tiempo.**
  - **Transacciones indebidas que logran atravesar el perímetro.**
- ***Mito: "La seguridad perimetral es estática".***





- **Magnitudes de tráfico.**

Criterios de Monitoreo y Control

Configuración de Nodos de Red

- Restricción de acceso administrativo a orígenes IP conocidos, identificados y controlados.
- AAA.
- Registros de actividad (“logs”).
- La configuración de estos parámetros debe ser controlada para asegurar su permanencia en el tiempo.

Gestión de la Infraestructura

- Esquema de mediación para centralizar el acceso y registrar actividad.
- Segmentación de redes.
- Control de acceso a la gestión de activos de servicio.
- Segregación de funciones.
- Monitoreo de ejecución de comandos sensibles en nodos críticos.

Criterios de Monitoreo y Control (cont.)

Detección de Actividad Inusual

- Monitoreo de accesos fallidos persistentes (“bruteforcing”).
- Cambios en registros de nuestros DNS.
- Reputación e integridad de recursos propios.
- Acceso a recursos corporativos o aplicativos de negocio desde países atípicos.
- Modificaciones en Firewalls perimetrales.

Criterios de Monitoreo y Control (cont.)

Detección de Actividad Inusual (cont.)

- **Bloqueos masivos de usuarios.**
- **Uso indebido de usuarios genéricos.**
- **Actividad de credenciales revocadas o suspendidas.**
- **Acceso a la gestión de elementos críticos desde esquema de mediadores.**
- **Cambios en la políticas de auditoría.**

Ataques contra Recursos de Misión Crítica

"DDoS" - Definición

- **Consisten en la saturación de un recurso informático (típicamente expuesto a Internet) o del vínculo de transporte del cual depende, desde múltiples orígenes, con el objetivo de dejarlo fuera de servicio.**

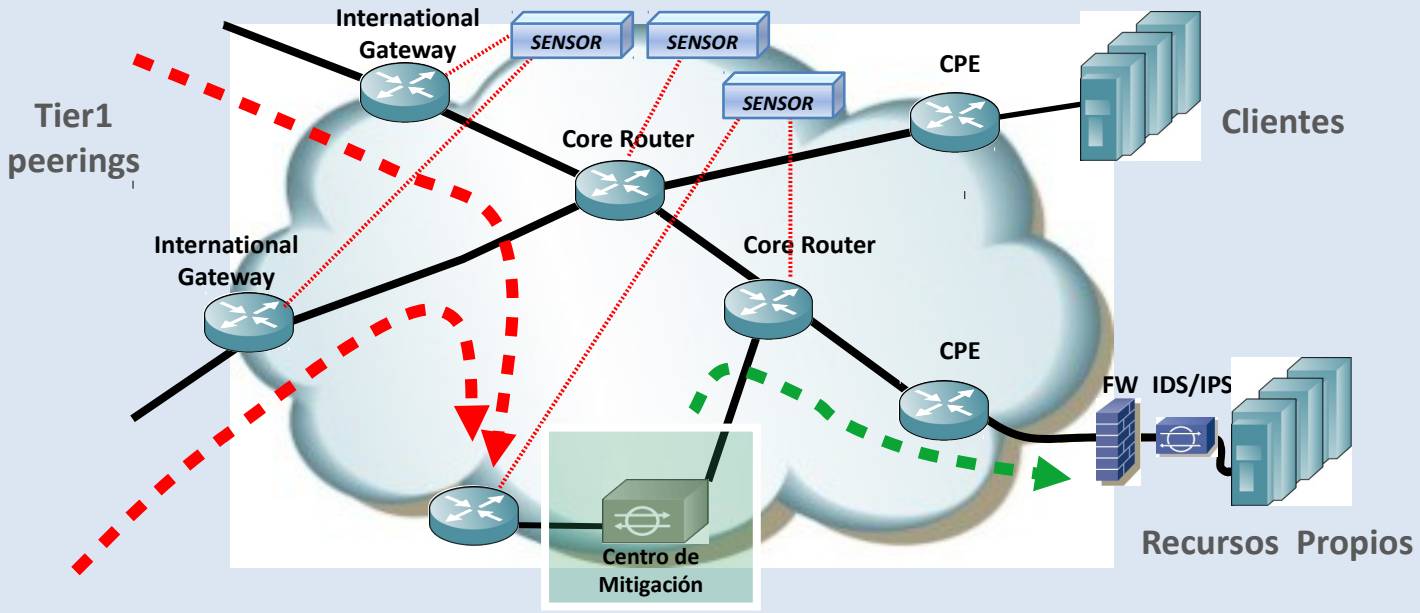
Aspectos Técnicos y Contexto

- **Suelen llevarse a cabo mediante la utilización de máquinas infectadas o "zombies", que conforman redes "botnets" sin conocimiento de sus propietarios legítimos.**
- **Actualmente, la participación en un ataque de DDoS no implica:**
  - **Intencionalidad**
    - ***botnets, malware, contenido incrustado en sitios web.***
  - **Conocimientos técnicos**
    - ***múltiples herramientas de libre acceso.***
  - **Ancho de banda saliente por parte del atacante**
    - ***Los ataques de amplificación reducen considerablemente el número de atacantes necesarios para causar un efecto negativo sobre el destino.***
    - ***Factores de amplificación de 1:100 son fácilmente alcanzables.***
    - ***Casos típicos DNS y NTP.***
- **Constituyen una tendencia creciente.**
- **Destinos habituales:**
  - **Infraestructura crítica (DNS, MX, nodos de red).**
  - **Sitios WEB, particularmente aquellos con contenido de connotación política o gubernamental.**

Ataques contra Recursos de Misión Crítica (cont.)

El Enfoque de Telecom Argentina

- Telecom Argentina cuenta con una solución que permite:
  - Detectar un ataque de DDoS.
  - Identificar el tráfico malicioso.
  - Desviarlo a un centro de filtrado y reinyectar sólo el tráfico legítimo al destino final, procurando asegurar su continuidad operativa.



Ataques contra Recursos de Misión Crítica (cont.)

El Enfoque de Telecom Argentina (cont.)

- Es utilizada para el resguardo de recursos propios, y de clientes externos suscriptos al servicio.
- Cuenta con capacidad de detección y mitigación en IPv4 e IPv6.
- Opera sobre Internet, y sobre MPLS-VPN.
  - *Ej.* detección y contención de ataques entre sitios de cliente vinculados por enlaces MPLS.
- El monitoreo de tráfico se basa en la inspección de magnitudes de volumen y características de su formación, mediante el análisis de los encabezados de los paquetes IP que lo conforman.

Magnitudes y Tendencias

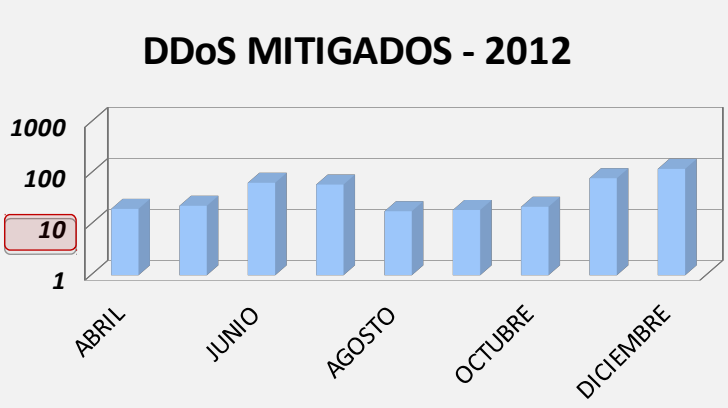
2012

Máximo 2 ataques diarios

2013

Promedio 12 ataques diarios

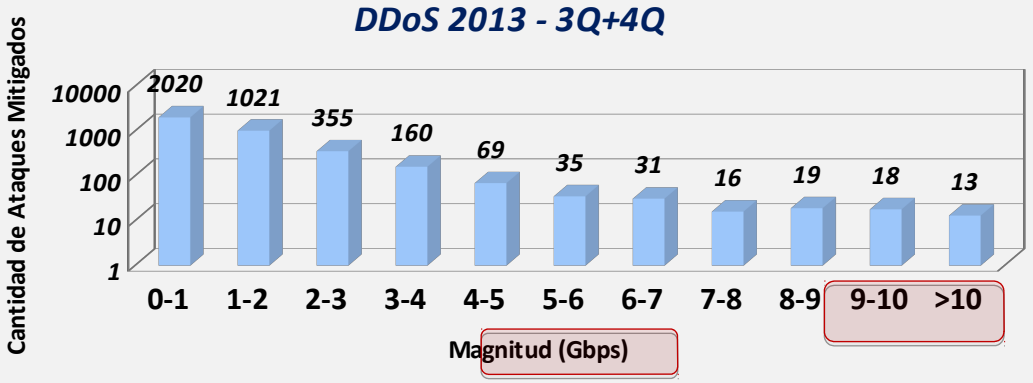
Máximo 140 ataques en 1 día



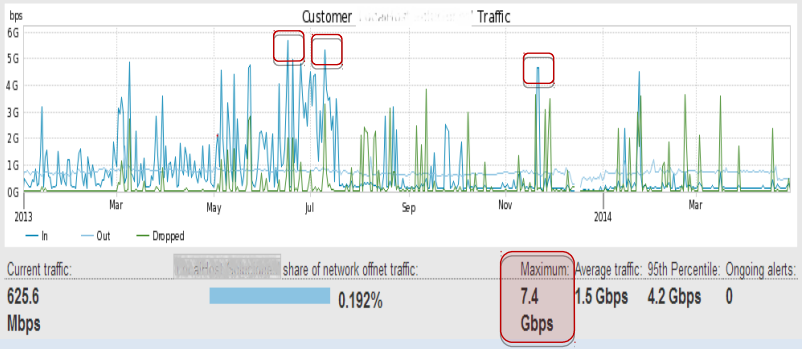
Ataques contra Recursos de Misión Crítica (cont.)

Magnitudes y Tendencias (cont.)

- **Más del 45% de los ataques superan el orden del Gbps.**
  - ***Cuántos clientes cuentan con enlaces que permitan hacer frente a este volumen…?***
- **Ataques de magnitudes superiores a los 10 Gbps son cada vez más frecuentes.**

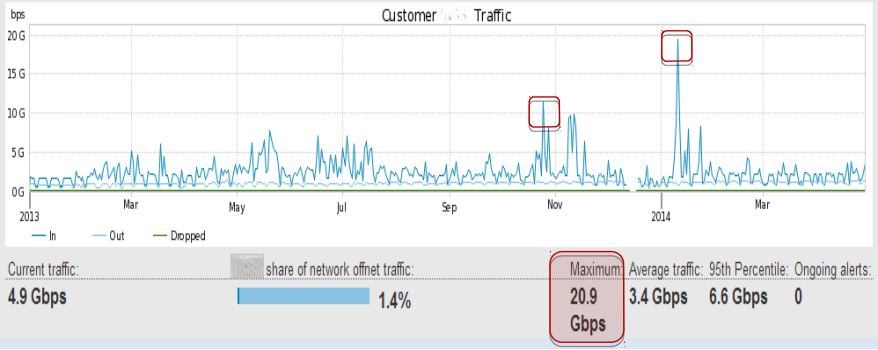


Caso real: cliente mayorista en Datacenter



Caso real: cliente mayorista con enlace de datos

Ataque > 20 Gbps



Hacktivismo

Casos Recientes de Público Conocimiento

SPAMHAUS

- **Marzo 2013.**

Ataque de DDoS sobre SPAMHAUS, cuyo impacto produjo disminución en el tráfico de internet de Europa. Fue realizado por Cyberbunker en represalia por haber sido sumado a la lista de "spammers".

The New York Times

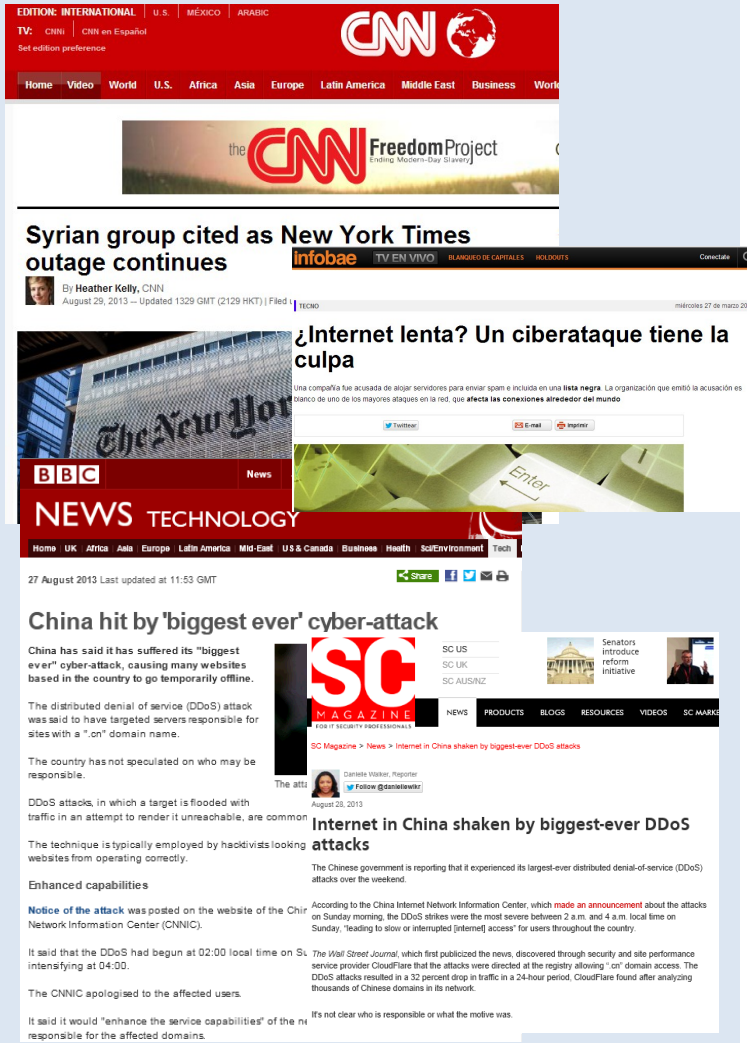
- **Agosto 2013.**

Un ataque de DDoS sobre el diario New York Times durante 20 horas, realizado por hacktivistas del Syrian Electronic Army debido a las presiones políticas de EEUU.

CNNIC

- **Agosto 2013.**

Ataque de DDoS a la entidad responsable de asignación de nombres de dominio ".CN" (CNNIC) paraliza durante 2 horas el servicio de Internet en China. Ningún grupo se atribuyó el ataque y se desconocen los motivos.



Hacktivismo (cont.)

Casos Recientes de Público Conocimiento (cont.)

- **Marzo 2013.**

American Express sufrió un ataque durante 2 horas y media, Chase Bank durante hora y media y también Wells Fargo. El grupo islámico de cyberactivistas "Izz ad-Din al-Qassam" se adjudicó el evento, en el marco de una serie de ataques contra entidades bancarias y financieras de Estados Unidos.


infobae TV EN VIVO OBAMACARE CIERRE DE GOBIERNO Conectate

RÁPIDO / CÓMODO / SEGURO credi click BANCO COMAFI abrir

NEGOCIOS viernes 29 de marzo 2013

Hackers atacan American Express

El ciberatentado **paralizó el portal de la empresa** de tarjetas de crédito durante más de dos horas. Días atrás, ocho bancos estadounidenses sufrieron sabotajes

NBC NEWS TECHNOLOGY

TOPICS Gadgets Security Internet Innovation More

HACKS Chase Bank site attacked, suffers intermittent outage

GRAND THEFT AUTO ONLINE 'Grand Theft Auto Online' off to a bumpy start

UHD TVS Cheap(er) 4K: Seiki's 65-inch Ultra HD set will sell for under $3,000

SCIENCE Sad about panda cam shutdown? Try these critter cams

Chase Bank site attacked, suffers intermittent outage

Devin Coldewey, NBC News

March 12, 2013 at 6:38 PM ET

Personal Business Commercial

CHASE

Products & Services Why Chase? Log In or Enroll

Our website is temporarily down, but our branches and Mobile Apps

The website of Chase Bank was inaccessible on Tuesday because of a denial-of-service attack. The initial service interruption to Chase.com lasted about 90 minutes, from about 5 to 6:30 p.m. ET.

When the site did load intermittently during

- **Febrero 2012.**

Ataque de DDoS durante 9 horas al sitio de la CIA y del estado de Alabama, el ataque fue realizado por Anonymus en represalia por una legislación contra inmigrantes ilegales.


10 Feb 2012 4:47pm, EST

Update: CIA site back up after Anonymous claims attacks on it and Alabama state sites

By M. Alex Johnson, Staff Writer, NBC News

Follow M. Alex Johnson on Twitter and Facebook

Updated at 11:45 p.m. ET: cia.gov is back up, although it is loading slowly, about nine hours after it was reported to be down, followed shortly by a claim that the hacker group Anonymous was responsible.

Updated at 7:10 p.m. ET: cia.gov remains inaccessible four hours after it was first reported to be down, followed shortly by a claim that the hacker group Anonymous was responsible. As security experts have noted, that's an unusually long time if the attack really is a straightforward DDoS assault.

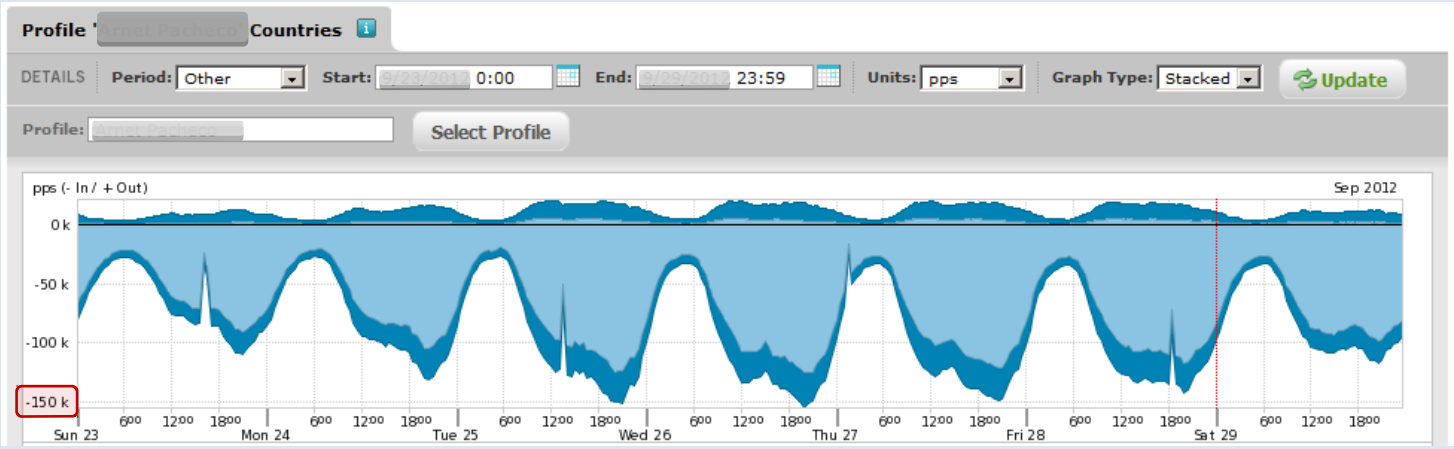
Meanwhile, the Anonymous Twitter account that set off the original round of

Hacktivismo (cont.)

Nuestros Recursos como Objetivo de Ataque

- **Bajo condiciones normales, Argentina concentra el 70% de los accesos hacia nuestros recursos expuestos a Internet.**

  (El intercambio contra EEUU incluye tráfico DNS y SMTP)

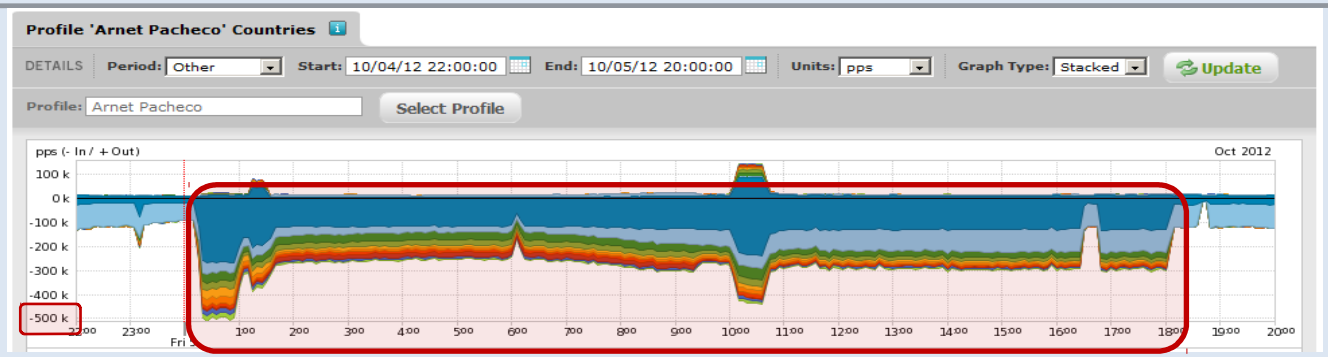


Country	% Total
Argentina	69.33%
United States	24.54%
Germany	0.62%
United Kingdom	0.61%

Hacktivismo (cont.)

Nuestros Recursos como Objetivo de Ataque (cont.)

- **Bajo ataque, el 81% del tráfico proveniente típicamente de más de 100 (cien) países geográficamente distribuidos incluyendo América del Norte, Asia y Europa del Este.**



Country	% Total
United States	32.96%
Argentina	19.22%
China	6.29%
Japan	4.20%
Germany	2.48%
United Kingdom	2.37%
Korea, Republic of	2.21%
Thailand	1.76%
Canada	1.53%
France	1.49%
Brazil	1.43%
Australia	1.32%
Italy	1.25%
Russian Federation	1.14%
Mexico	1.06%
Netherlands	0.91%
Taiwan	0.87%
Spain	0.76%

Country	% Total
Spain	0.76%
India	0.70%
Indonesia	0.62%
Chile	0.55%
Sweden	0.49%
Poland	0.47%
Europe	0.45%
Switzerland	0.43%
Turkey	0.37%
Uruguay	0.37%
Colombia	0.34%
South Africa	0.34%
Austria	0.31%
Hong Kong	0.30%
Ukraine	0.30%
Vietnam	0.30%
Romania	0.29%
Norway	0.27%
Denmark	0.26%

Country	% Total
Denmark	0.26%
Czech Republic	0.24%
Finland	0.23%
New Zealand	0.21%
Belgium	0.19%
Pakistan	0.17%
Venezuela	0.17%
Israel	0.16%
Singapore	0.16%
Malaysia	0.16%
Hungary	0.15%
Greece	0.14%
Bulgaria	0.13%
Portugal	0.13%
Egypt	0.13%
Ireland	0.12%
Philippines	0.10%
Saudi Arabia	0.09%
Iran, Islamic Republic of	0.09%

Country	% Total
Costa Rica	0.09%
Peru	0.08%
Lithuania	0.07%
Guatemala	0.06%
Slovakia	0.06%
Panama	0.06%
Latvia	0.05%
Kazakhstan	0.05%
United Arab Emirates	0.05%
Ecuador	0.05%
Morocco	0.05%
Slovenia	0.05%
Serbia	0.05%
Croatia	0.04%
Nepal	0.04%
Algeria	0.04%
Tunisia	0.04%
Luxembourg	0.03%

Country	% Total
Kenya	0.03%
Kuwait	0.03%
Bangladesh	0.03%
Bolivia	0.03%
Estonia	0.03%
Belarus	0.03%
Puerto Rico	0.03%
Iceland	0.02%
Satellite Provider	0.02%
Moldova, Republic of	0.02%
Bosnia and Herzegovina	0.02%
Nigeria	0.02%
Paraguay	0.02%
Georgia	0.02%
Dominican Republic	0.02%
El Salvador	0.01%
Qatar	0.01%
Lebanon	0.01%

Monitoreo y Protección de Infraestructura Crítica

¿ Preguntas ?

Gracias,