

Telefónica: Seguridad en las Comunicaciones



Marzo 2011

Telefónica España – Grandes Clientes

Juan Miguel Velasco

Gerente de Desarrollo de Negocio

Telefonica

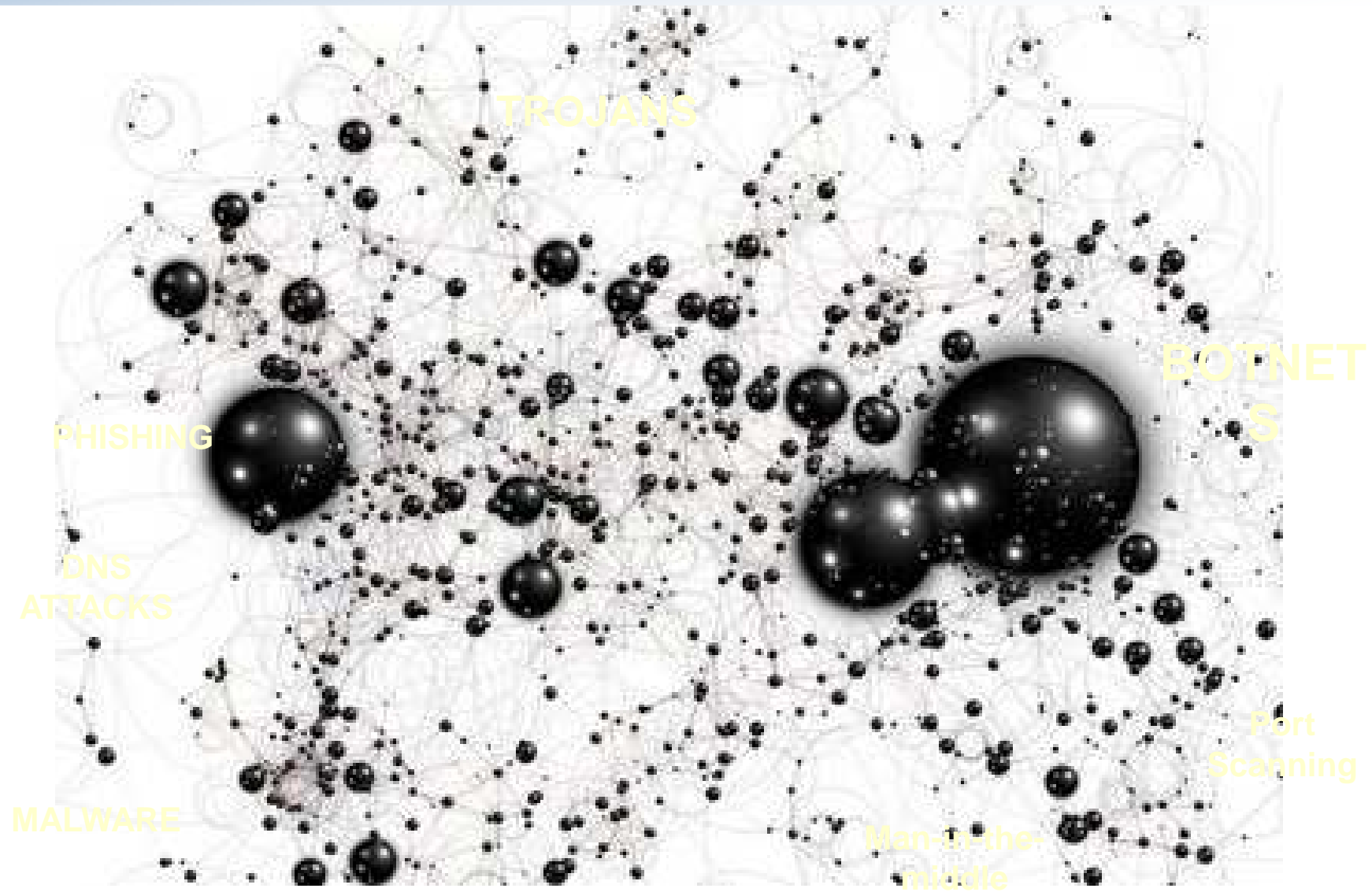
Índice


1. ¿QUÉ HAY EN LA RED?
2. Objetivos y Retos de Telefónica para el 2011
3. Conclusiones

01

Que hay en la red?

Están nuestras redes repletas de basura?





Más del 18% del tráfico en las redes IP está relacionado con los ataques, malware o tráfico no deseado ... **y más del 80%** de los ordenadores están infectados con algún tipo de malware

Servicio de Correo Limpio

Evolución correos procesados 2004 – Diciembre

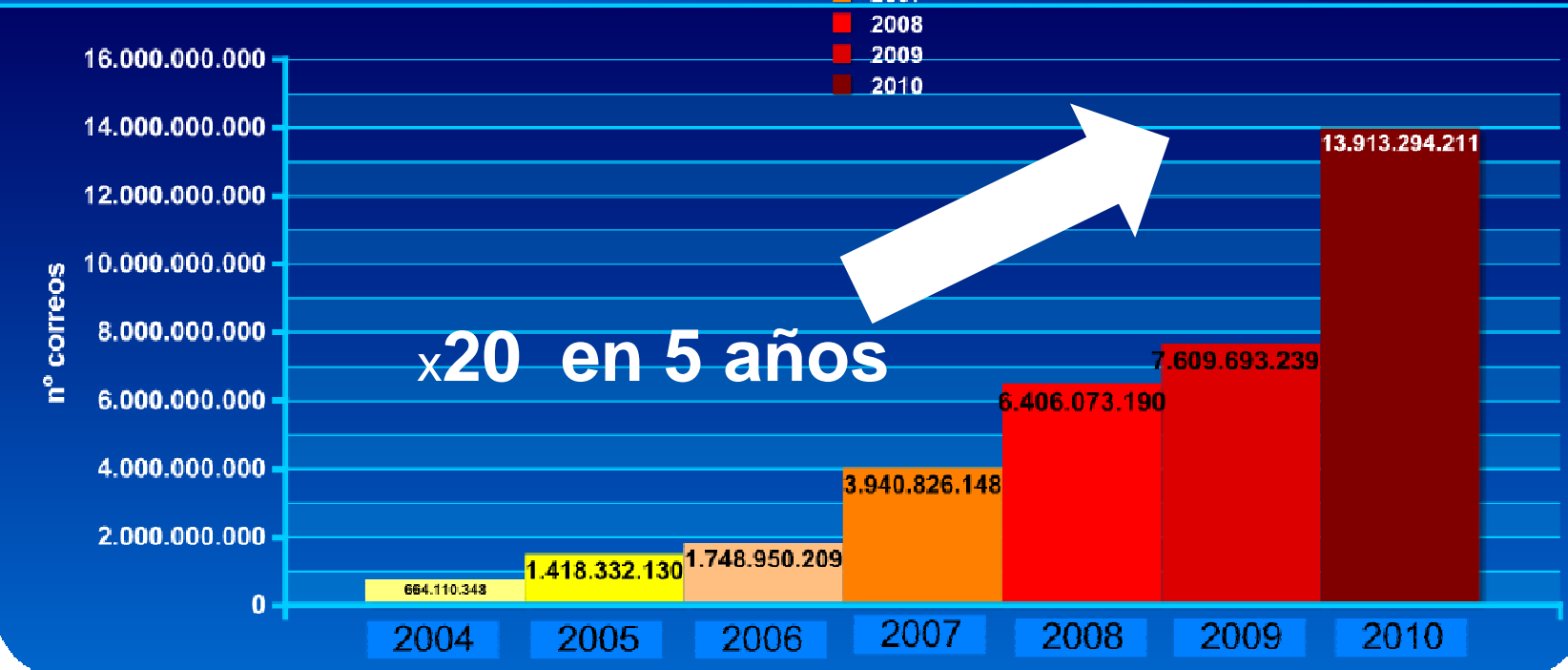
2010

Correo recibido

2004 / Diciembre 2010 (Servicio correo TEE)

- 2004
- 2005
- 2006
- 2007
- 2008
- 2009
- 2010

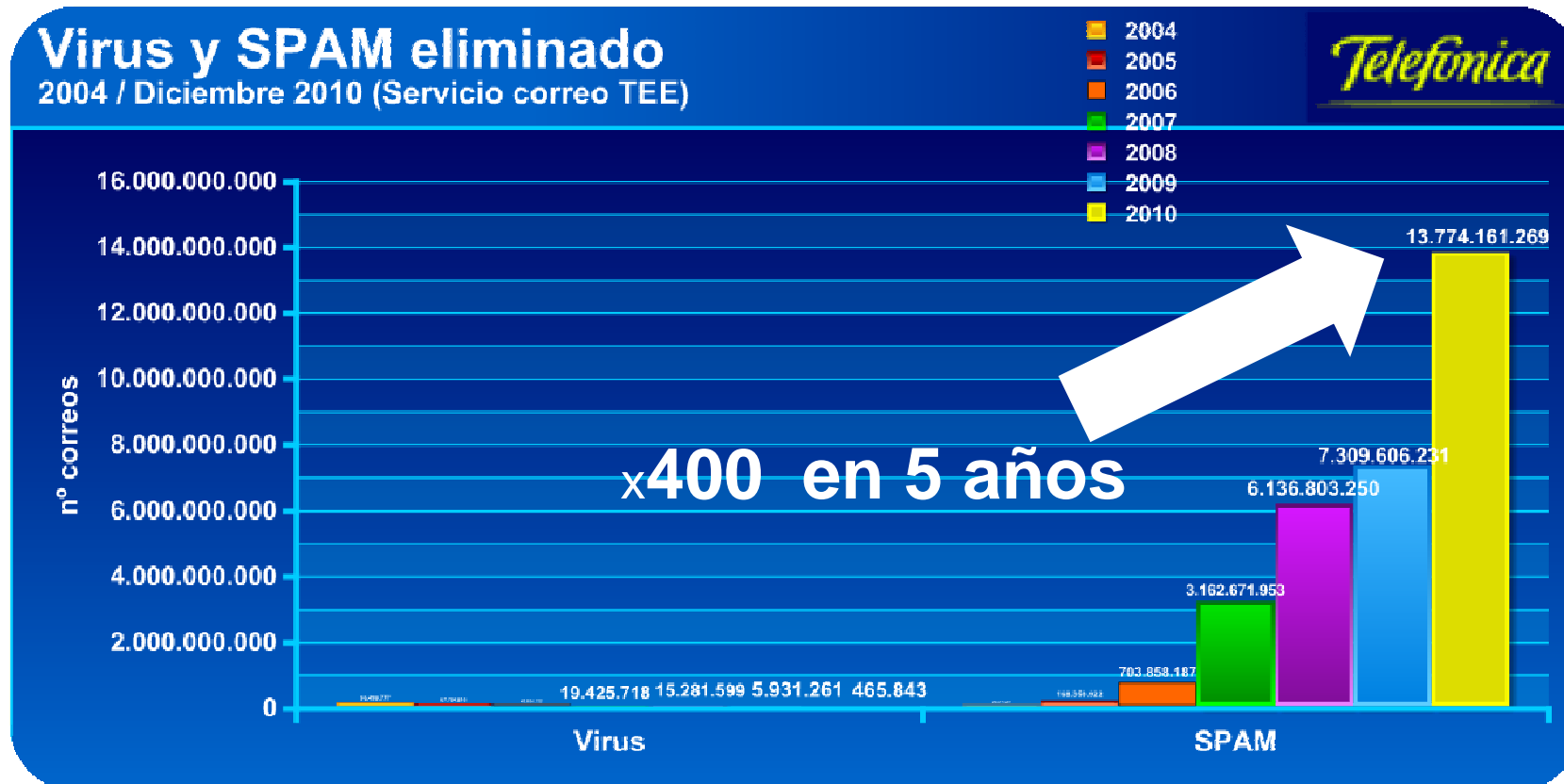
Telefónica



A lo largo del año 2010 se confirma el ascenso en el volumen de correo procesados. Se ha pasado de 600 Mill en 2004 a casi 14.000 Mill en 2010

Servicio de Correo Limpio

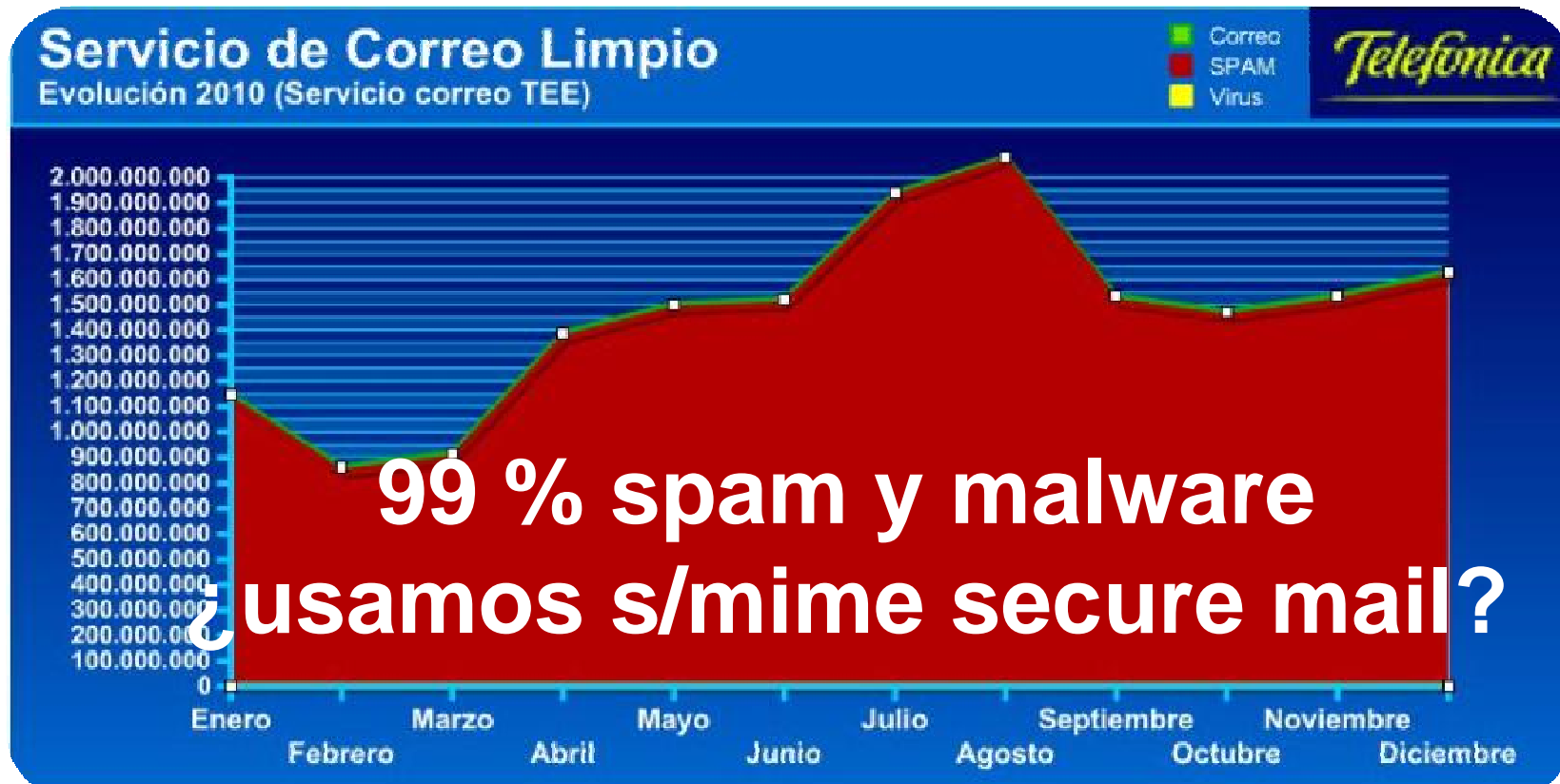
Virus y SPAM eliminado 2004 – Diciembre 2010



A mediados del 2010 el SPAM ya había superado el total del año 2009.

Servicio de correo limpio

Evolución 2010

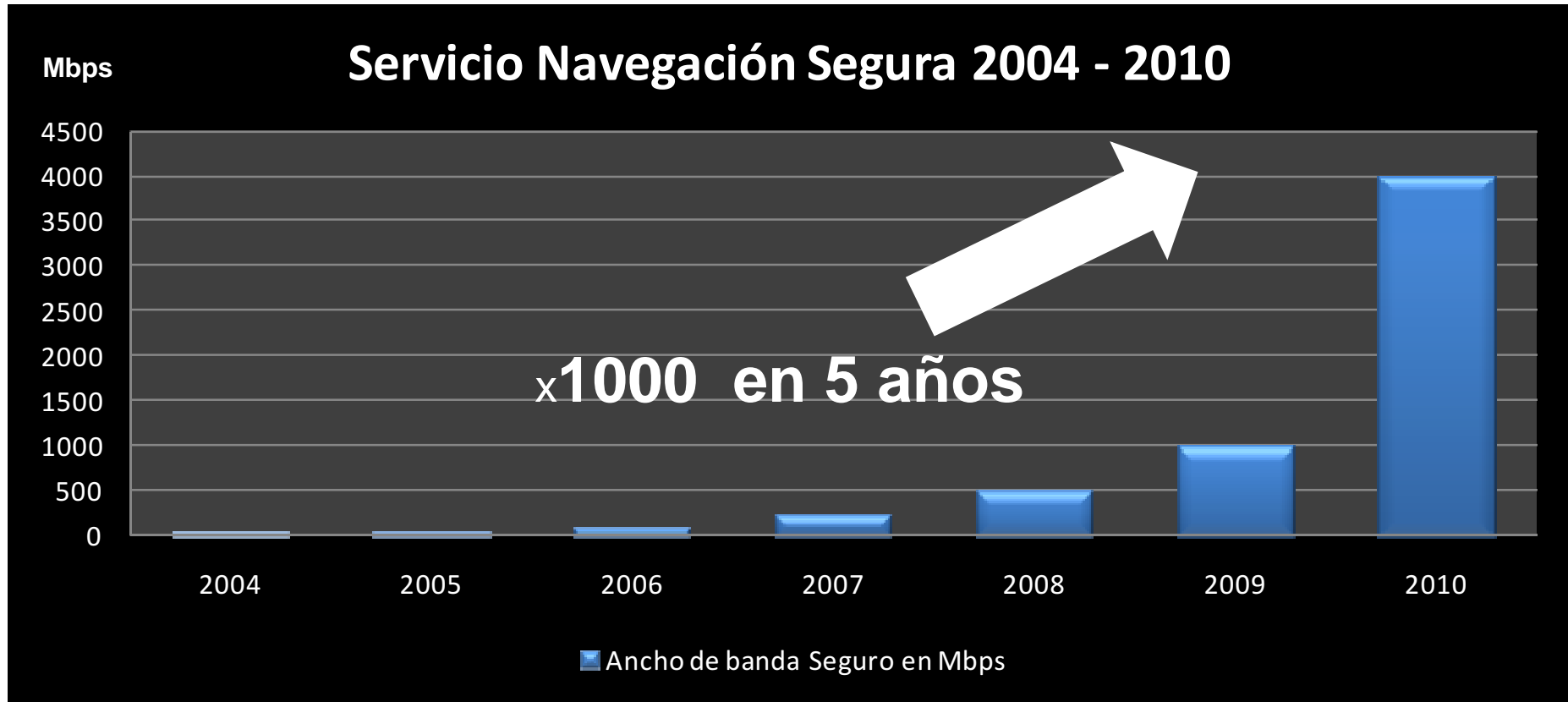


Durante el 2010 el nivel de SPAM sigue en el 99% de todo el correo recibido, aproximadamente 1 email válido por cada 100 procesados.

Sin contar reputacional IP

Servicio Navegación Segura

Ancho de banda gestionado 2004 – Diciembre 2010

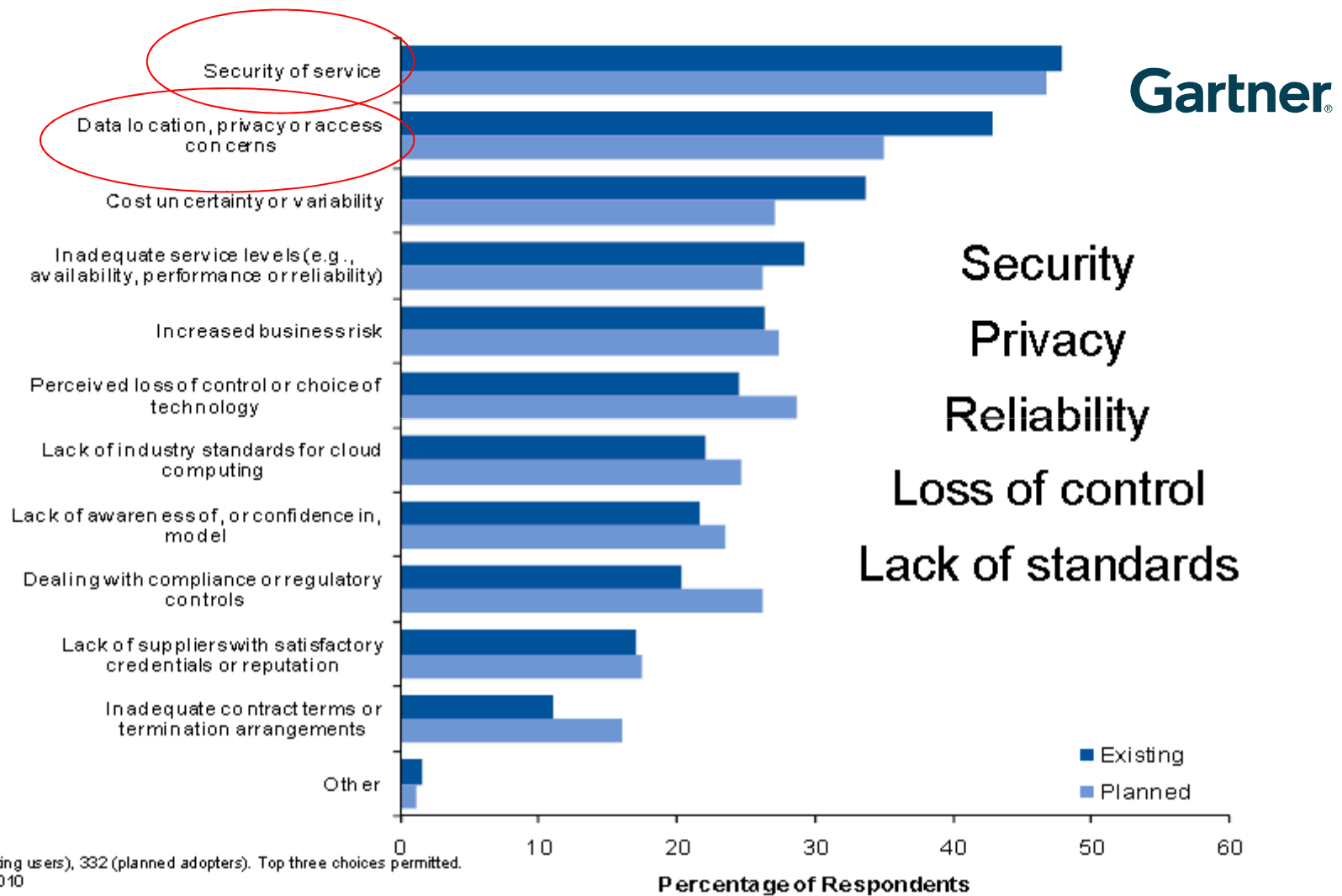


En Diciembre 2010 se alcanzó la capacidad de 4 Gbps de caudal de capacidad agregada para todos nuestros clientes de Redes Limpias o Servicio de Navegación Segura, que es más de 1000 veces la capacidad inicial del servicio en 2004

02

Objetivos y Retos de Telefónica para el 2011

Key Concerns When Adopting Cloud Computing



What Control Mechanisms Does the Vendor Provide?

- **Identity and access management**
 - Federation, strong authentication, access and roles
 - How to verify who has access to what and who has done what?
- **Data confidentiality protection**
 - Encryption of data at rest and in transit
 - How do you manage encryption keys?
- **Monitoring and alerting**
 - DLP, IPS, SoD, DAM
 - How do you perform an audit?
- **Discovery and investigation**
 - How do you do forensics in multiple jurisdictions?
 - What is a business record?
 - Don't forget law enforcement access



If they don't build it in, you can't use it.

Gartner.

Los retos del CLOUD Seguridad en 2011...

Proteger el Cloud y su uso seguro



- Proteger el perímetro del Cloud
- Controlar los datos y la información que manejan los proveedores Cloud
- Cumplir con la Legislación local y la multi-regional cuando se usan servicios Cloud
- Inversión o gasto en el Cloud, cambio del modelo de gestión
- Control, administración, reporting , provisioning y billing en Cloud
- Gestionar los SLAs del Cloud

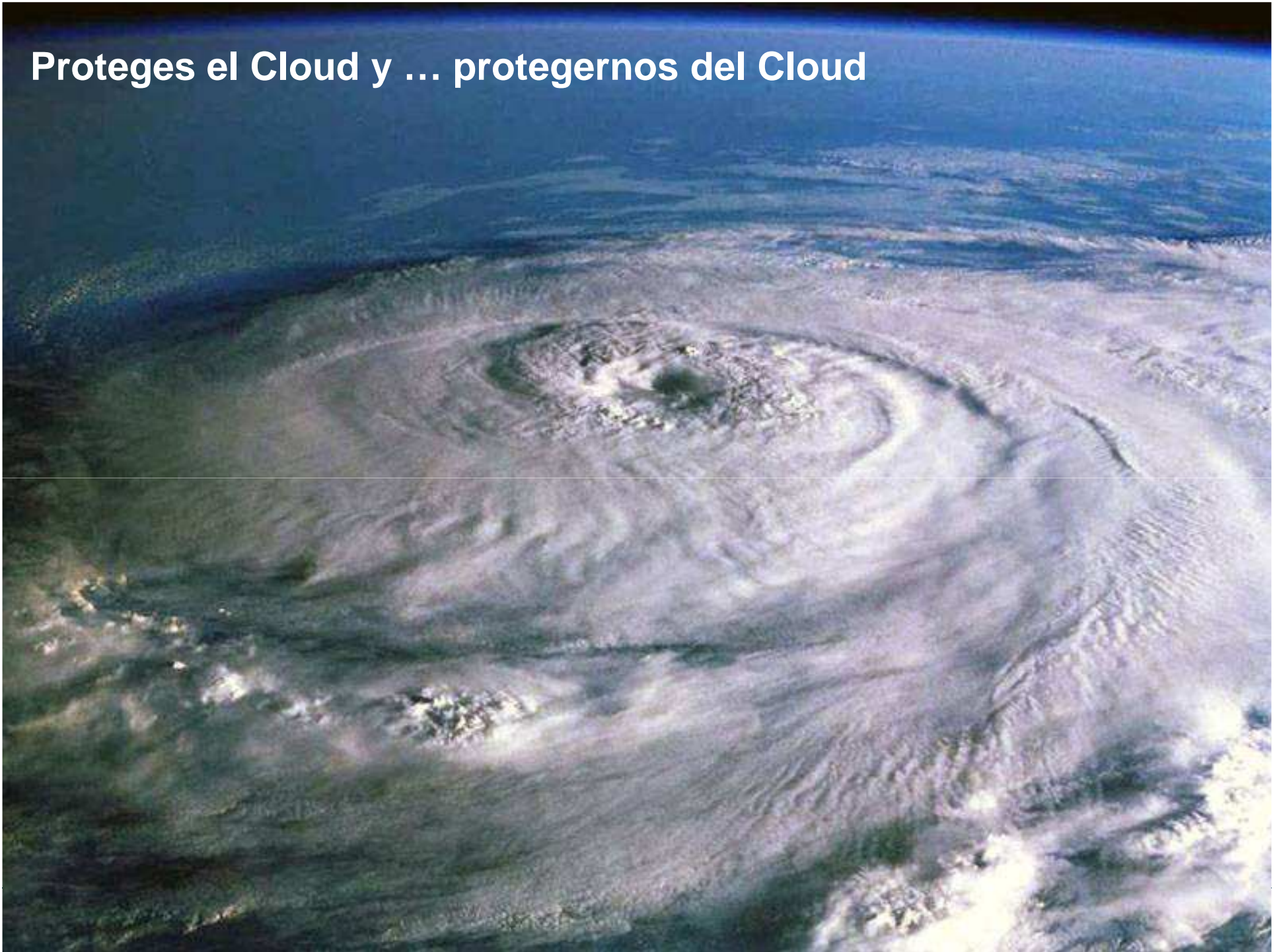
...usar el Cloud para nuestra protección ...

El Cloud Seguridad y protegernos del Cloud



- Servicios de Redes Limpias maduros multidispositivo, ubicuos, rápido despliegue, poca inversión y pago por uso
- Inteligencia en RED, utilizar la compartición anónima de información de fraude, ataques y correlación -> Correlación en Cloud.
- Servicios Seguridad virtual dentro del perímetro de servicios Cloud de infraestructuras
- Protección de ataques en Cloud -> sólo con Servicios de Seguridad
- El uso del “bad cloud” , botnets, DDoS, hacking, phishing, smishing, etc.

Proteges el Cloud y ... protegernos del Cloud



Seguridad en los servicios CLOUD

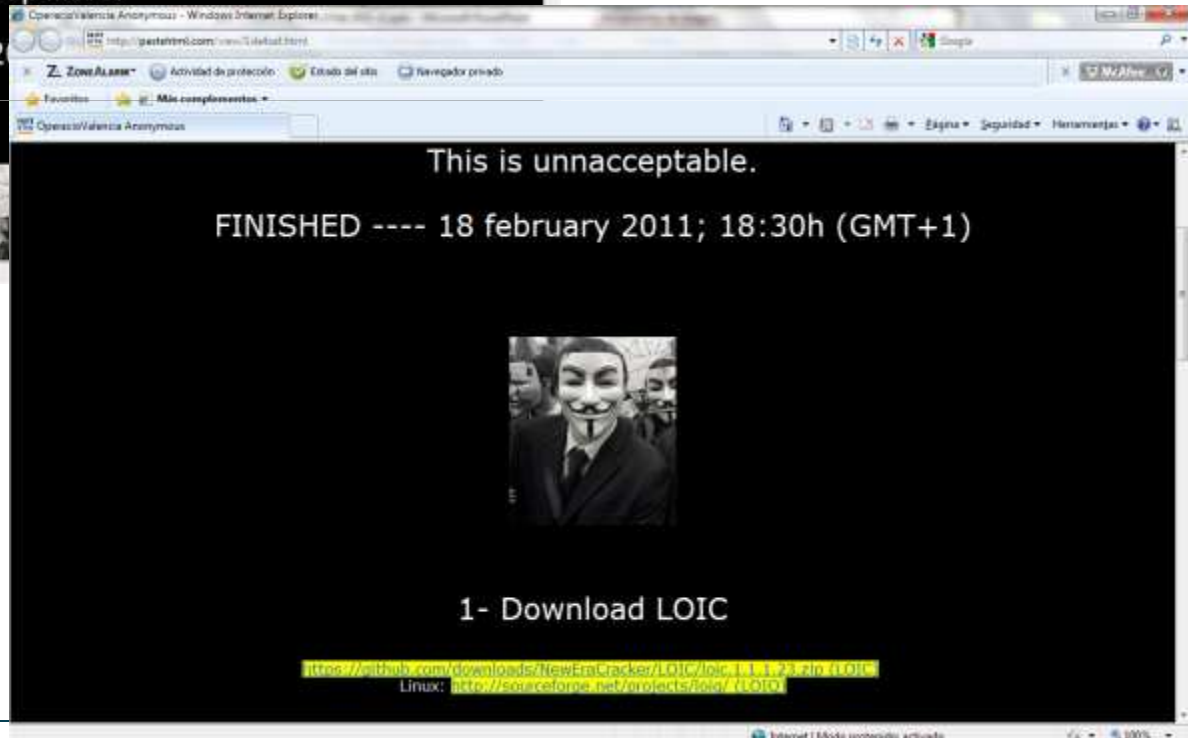
Proteger el Cloud y su uso seguro



- Autenticación fuerte Cliente - Servidor
- Cifrado de datos almacenados en el Cloud
- Garantía de integridad de datos
- Procesos de firma para autenticación y contratación de servicios en línea
- Autenticación fuerte multidispositivo sobre X.509v3
- Cifrado de dispositivos móviles
- Cifrado de aplicaciones
- Sistemas de doble factor de autenticación

¿es la seguridad un inhibidor de servicios cloud?

Estamos en medio.... Queramos



..... O no queremos y lo siguiente....

2 - Configure as described:

Low Orbit Ion Cannon

Manual Mode (On 4 years old) | IRC Mode (Disabled) | IRC server: [] Port: [] Channel: [] Disconnect

1. Select your target

URL: http://www.gva.es [Link OK] [Link OK]

2. Ready?

Selected target: **195.77.16.26** **OBJETIVO**

3. Attack options

TCP/UDP message: VOLUNTARIOS

HTTP Subsite: /

Append random chars to the subsite / message

Method: [] Port: [] Threads: [] Thread: [] Wait for reply: Wait for reply (HTTP)

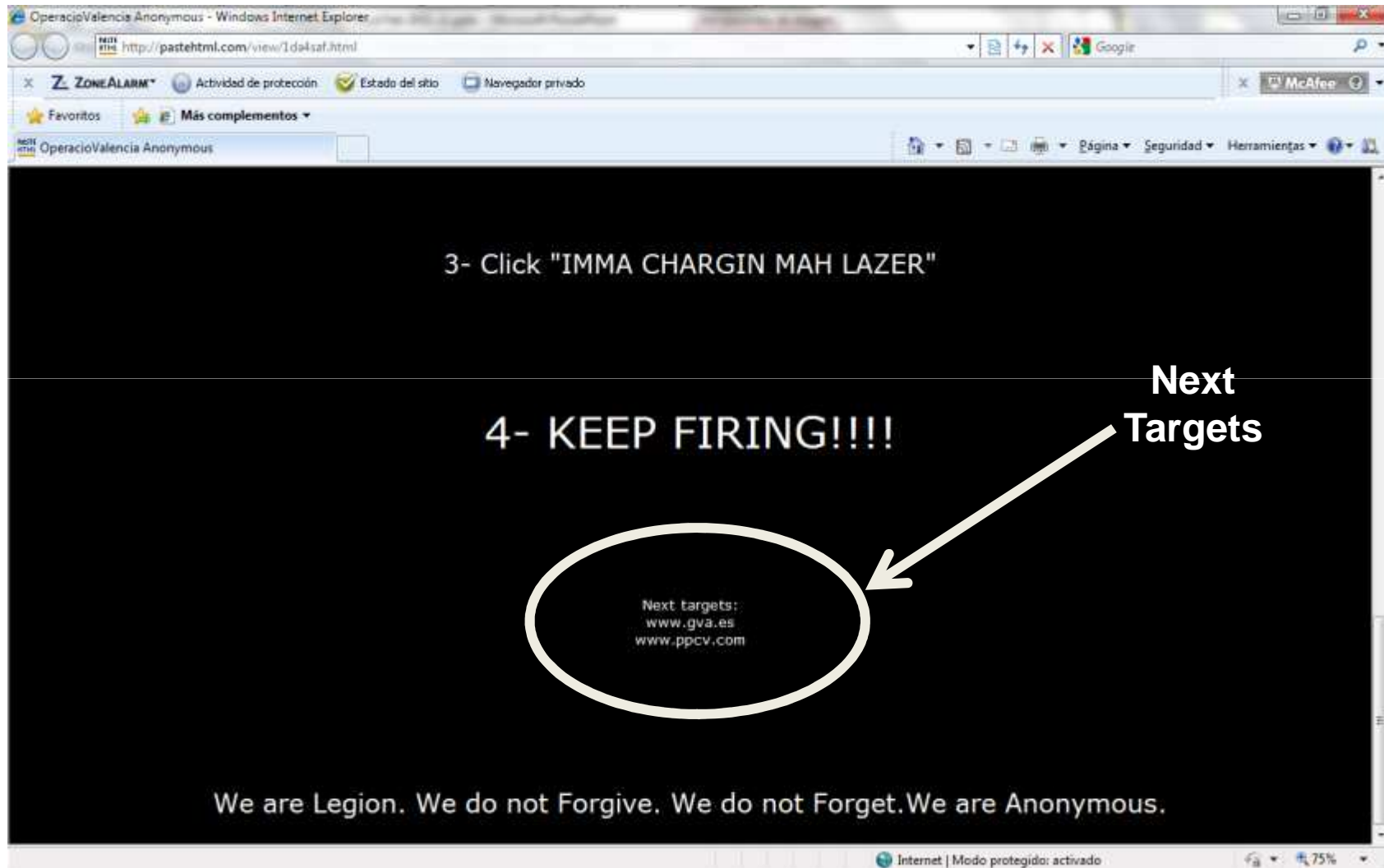
Attack status

| URL | Connection | Downloaded | Upload | Failed |
|-------------------|------------|------------|--------|--------|
| http://www.gva.es | Connecting | | | |

URL: http://www.gva.es
TCP port 80
Disable wait for reply

Internet | Modo protegido: activado | 75%

..... next steps..... **Cualquier! Cualquiera! TODOS!**



Ataque DDoS Ideológicos

En el mundo físico:



En Internet:

- Herramientas donde sólo tienes que elegir un objetivo y hacer “click”
 - LOIC, LOIQ, JS LOIC
 - HOIC
 - GOIC





ANONYMOUS

Comunicado de Anonymous para la Operación Hipoteca

Desde Ar
abusos i

Asistimos

El gobier
sienta e

Casos cor
pre gana
que se

Propuesta
el PSOE, l
a las dac
blico en c:

Mientras
gran núm
etc., y se
para q

Aún así,
cuidan s
Aznar c:
tranquila
tir el paste
beneficio



ANONYMOUS



BASTA YA!

Durante años el Gobierno y la Banca se reparten lo que ha quedado de la explosión de la burbuja inmobiliaria

UNETE A
ANONYMOUS
#ophipoteca



IRC
<http://anono.ps/hispano>
URL
www.anonymous-spain.es



ayudando a un grupo de 6.340 millones de euros en 2009, el BBVA 4.210 millones, La Caixa 1.510 millones y no fueron los únicos).



ANONYMOUS

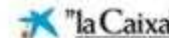
El Gobierno no se reúne con los Autonomos, con los trabajadores, Con los de a Pie...



dedica todos sus esfuerzos a umentar el Beneficio de sus ccionistas

UNETE A
ANONYMOUS
#ophipoteca

IRC
<http://anono.ps/hispano>
URL
www.anonymous-spain.es



Y a SONY-playstation qué le ha pasado?

- Caída en bolsa por el ataque

-3,82%

Valor

-1.130 Mill

**Servicios y RED
caídos 1 semana**

VIDEOJUEGOS | PlayStation Network

Sony admite que un intruso accedió a datos de millones de usuarios de PlayStation

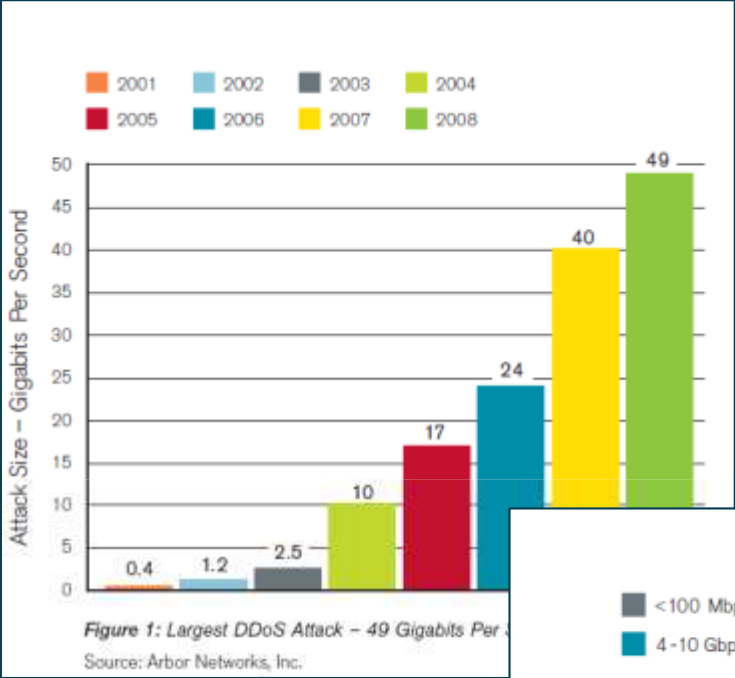
- Sony asegura que no hay indicios de que hayan usado las tarjetas de crédito
- No obstante, ya se han dado las primeras denuncias de cargos fraudulentos
- En España hay 3.000.000 de cuentas de PSN y 330.000 con tarjeta de crédito
- Anonymous niega ser responsable de la intrusión entre el 17 y el 19 de abril



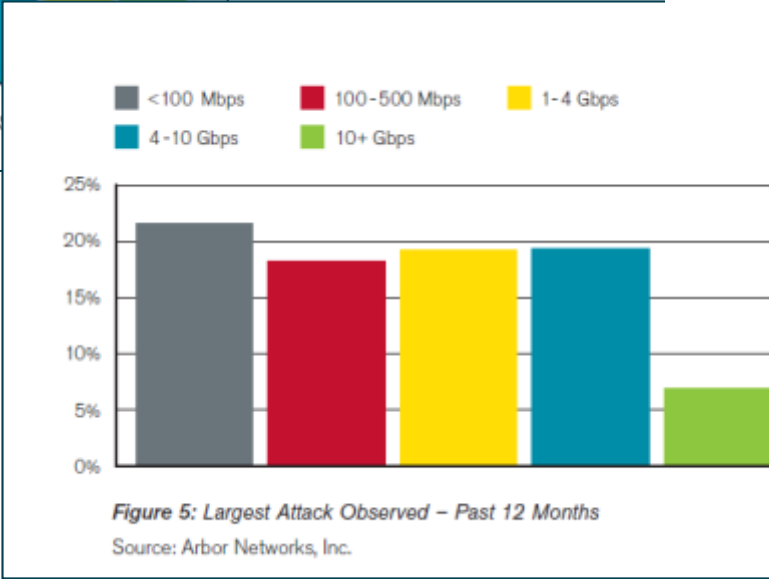
The screenshot shows the PlayStation Blog interface. At the top, there's a navigation bar with the PlayStation logo, the text 'PlayStation.Blog', and platform filters for PS3, PSP, and PSN. Below the navigation is a large banner image for 'KILLZONE 3 // UPDATES'. The main content area features a post titled 'Update on PlayStation Network and Qriocity' dated April 26, 2011, posted by Patrick Seybold. The post text reads: 'Thank you for your patience while we work to resolve the current outage of PlayStation Network & Qriocity services. We are currently working to send a similar message to the one below via email to all of our registered account holders regarding a compromise of personal information as a result of an illegal intrusion on our systems. These malicious actions have also had an impact on your ability to enjoy the services provided by PlayStation Network and Qriocity including online gaming and online access to music, movies, sports and TV shows. We have a clear path to have PlayStation Network and Qriocity systems back online, and expect to restore some services within a week. We're working day and night to ensure it is done as quickly as possible. We appreciate your patience and feedback.'

Detalle del tráfico

Tamaño de los ataques de denegación de Servicio



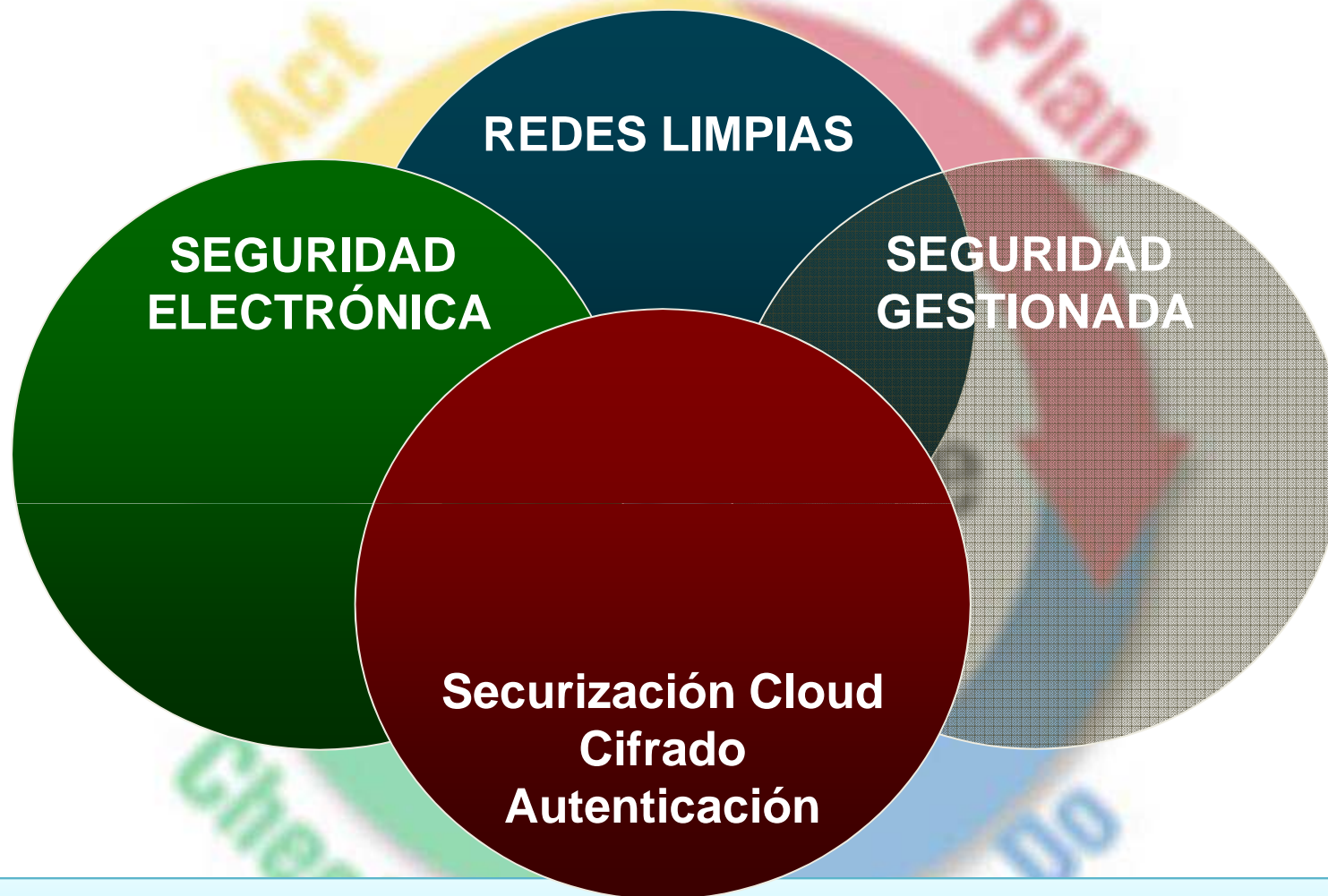
Capacidad media actual de ataque
 Ataque pequeño < 25 Mbps
 Ataque mediano < 100 Mbps
 Ataque grande > 100 Mbps



03

Conclusión

En resumen...



MIX de Servicios Remotos e INSITU / con ahorro de Costes por Gestión Integral / Integración con CGPs ORO / Apalancamiento en Comunicaciones / Apoyándonos en el CLOUD

Telefonica
