



**IX JORNADA  
de SEGURIDAD  
INFORMATICA**  
Monitoreo y Evolución de  
la Inseguridad Informática  
Junio 17, 18 y 19 de 2009

# EVOLUCIÓN DEL FRAUDE EN INTERNET

Jaime E. Gómez H. MSc. PhD.

Iván Darío Tovar R





# Agenda

- Historia
- Estado Actual
- Evolución
- Futuro
- Conclusiones



# Por qué Internet

Para el usuario:

- Más rápido: no tiene que desplazarse, ni hacer fila para que lo atiendan
- Mucho más cómodo: puede hacer transacciones a cualquier hora y desde cualquier lugar
- Mas barato: normalmente las transacciones son gratuitas o mucho menos costosas que en oficina o ATM

Para las entidades:

- Ofrece un mejor servicio al cliente
- Una transacción por Internet le cuesta mucho menos que una en oficina o en

ATM

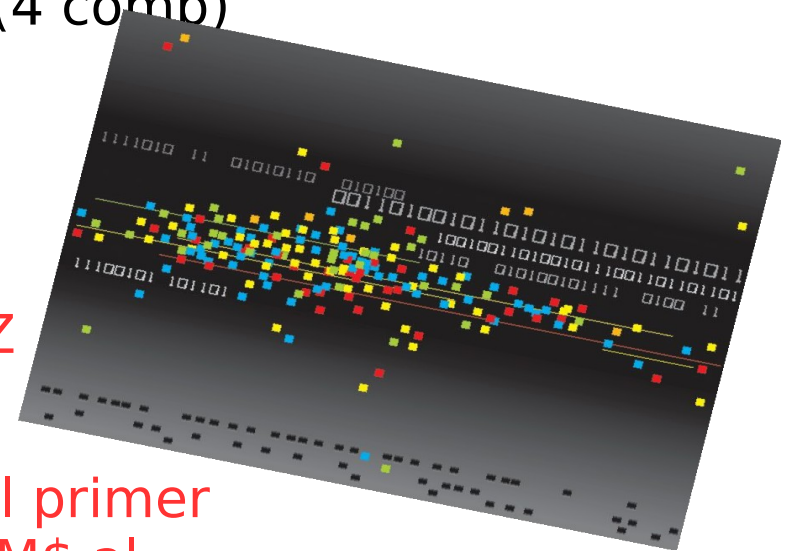




# Historia

## Internet Milestones

- 1836: Telegraph
- 1969: Arpanet nace. Nodo UCLA (4 comp)
- 1971: E-mail es inventado
- 1982: Establecido TCP/IP
- **1987: Nace el virus Vienna**
- **1989: Nace el gusano WANK/OILZ**
- 1991: Cern Publica WWW
- **1994: Nacen el primer Sniffer y el primer robo bancario (Vladimir Levin – 10M\$ al Citibank)**
- **1995: Nace el Spyware (fuente Wikipedia)**





# Peligros

- Robo de identidad
- Robo de información





# Como Roban

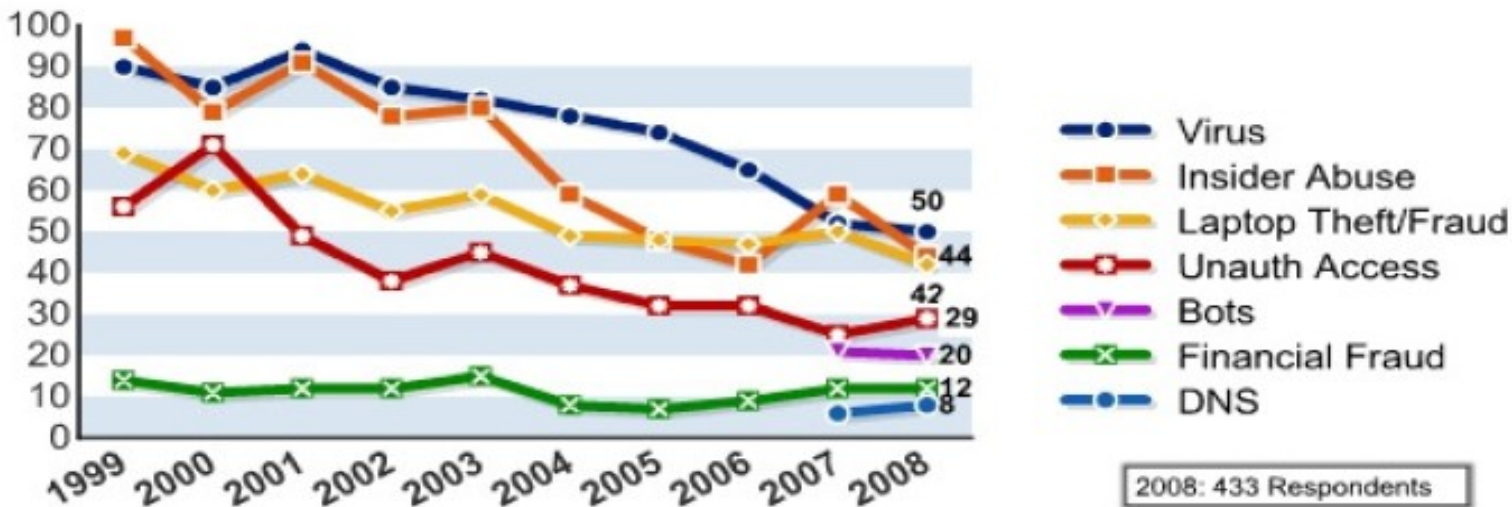
- Vulnerabilidades locales:
  - Loggers
  - Troyanos
  - Spyware genérico
- Vulnerabilidades remota
  - Phishing
  - Sniffing remoto
  - Man-in-the-Middle





## 2008 CSI Computer Crime and Security Survey

Figure 13: Percentages of Key Types of Incident





# Comportamiento

Table 1	2004	2005	2006	2007	2008
Denial of service	39%	32%	25%	25%	21%
Laptop theft	49%	48%	47%	50%	42%
Telecom fraud	10%	10%	8%	5%	5%
Unauthorized access	37%	32%	32%	25%	29%
Virus	78%	74%	65%	52%	50%
Financial fraud	8%	7%	9%	12%	12%
Insider abuse	59%	48%	42%	59%	44%
System penetration	17%	14%	15%	13%	13%
Sabotage	5%	2%	3%	4%	2%
Theft/loss of proprietary info	10%	9%	9%	8%	9%
from mobile devices					4%
from all other sources					5%
Abuse of wireless network	15%	16%	14%	17%	14%
Web site defacement	7%	5%	6%	10%	6%
Misuse of Web application	10%	5%	6%	9%	11%
Bots				21%	20%
DNS attacks				6%	8%
Instant messaging abuse				25%	21%
Password sniffing				10%	9%
Theft/loss of customer data				17%	17%
from mobile devices					8%
from all other sources					8%

Los fraudes referentes al robo de identidad o información se mantienen constantes, a pesar de las nuevas técnicas de defensa





# Evolución

## Spear Phishing

- Ataque a un grupo de personas específico
- Mensajes incluyen información personal
- Alto nivel de éxito
- Utilizan información de redes sociales y de bases de datos comprometidas (SalesForce.com)





## Spear Phishing - Whaling

- Ataque a un nivel específico de la organización
- Dirigido al nivel ejecutivo de la organización

Here is part of what the bogus email says:

--- Begin bogus email ---

Issued to: (Individual's name and title inserted here)

SUBPOENA IN A CIVIL CASE Case number: 94-621-PGM United States District Court

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below ...

Please download the entire document on this matter (follow this link) and print it for your record.

This subpoena shall remain in effect until you are granted leave to depart by the court or by an officer on behalf of the court ...

Failure to appear at the time and place indicated may result in a contempt of court citation ...

--- End bogus email ---



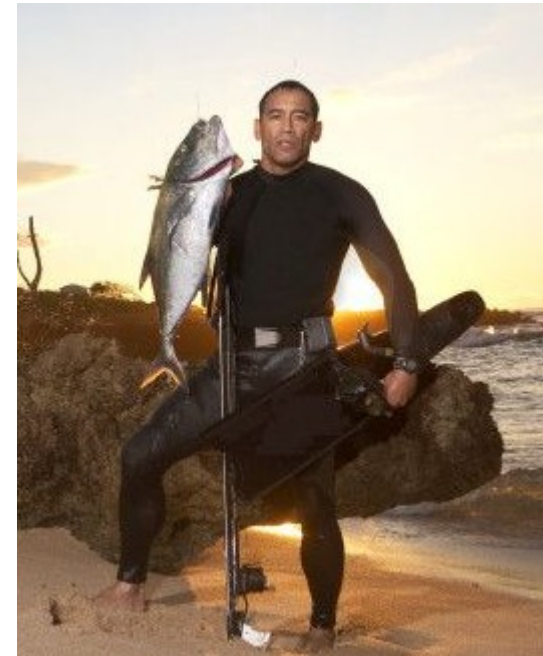
## Spear Phishing – Efectividad

Gartner: phishing tradicional

- 19% hace click en el link
- 3% entrega información personal

Academia militar West Point

Correo electrónico de un Coronel a los cadetes: **80%** entrega información personal o confidencial





# Evolución

- Vishing – Phishing en VoIP
  - Utilizando correo
  - Utilizando teléfono
- Llamadas usando un WarCaller
- Contestador automático refiere a otro número (ID de la entidad)
- Víctima llama y le piden tarjeta de crédito, expiración, PIN, etc)
- Ahora el delincuente tiene todos los datos necesarios para el fraude

**CHASE** 

Dear Customer,

We've noticed that you experienced trouble logging into Chase Online Banking.

After three unsuccessful attempts to access your account, your Chase Online Profile has been locked. This has been done to secure your accounts and to protect your private information. Chase is committed to make sure that your online transactions are secure.

To verify your account and identity please call our Account Maintenance Department at **(706) 247-7801** 24 hours / 7 days a week.

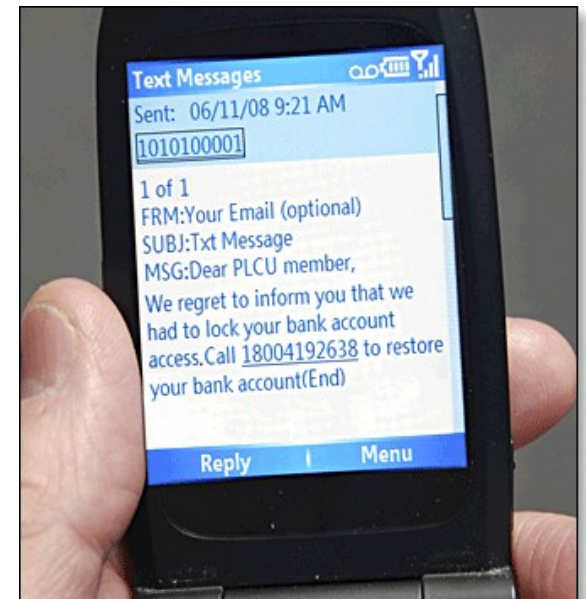
Sincerely,

Chase

Online Customer Service

## SMishing - Phishing en SMS

- SMS confirmando una compra o una transacción
- Solicitan una comunicación inmediata
- Engañan al usuario para obtener información o credenciales de autenticación





## Pharming

The screenshot shows a Windows XP file explorer window with the address bar set to `C:\WINDOWS\system32\drivers\etc`. The file list contains the following entries:

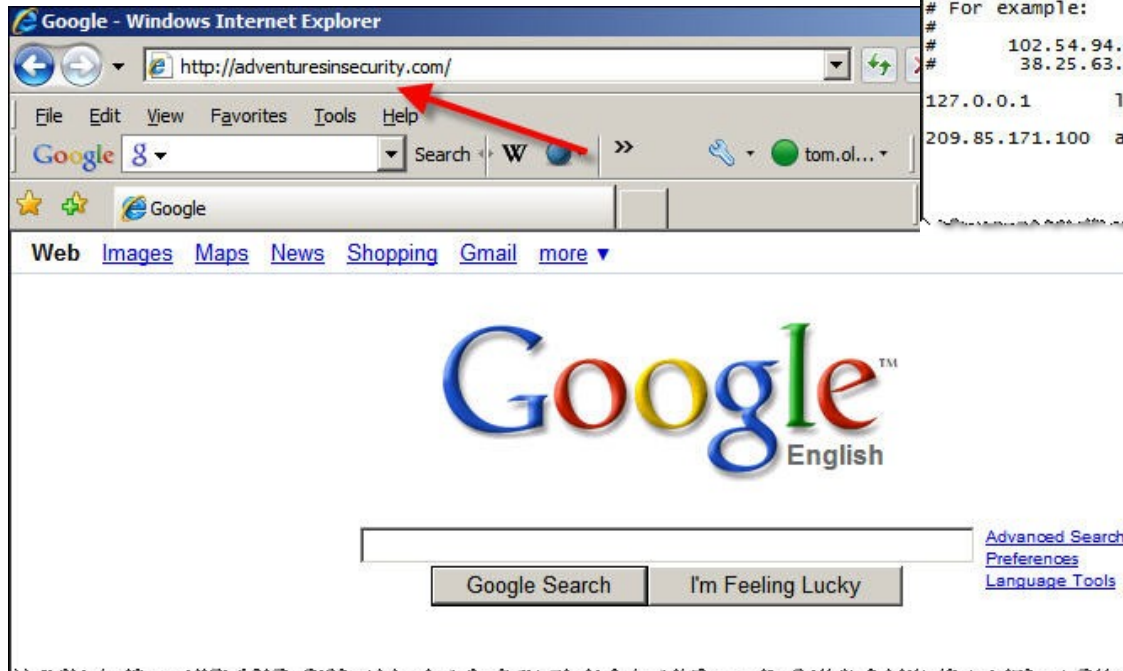
Name	Date Modified
hosts	10/26/2008
lmhosts.sam	8/4/2004 7:00
networks	8/4/2004 7:00
protocol	8/4/2004 7:00

The inset window, titled "hosts - Notepad", displays the following text:

```
File Edit Format View Help
# Copyright (c) 1993-1999 Microsoft Corp.
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
# For example:
#         102.54.94.97       rhino.acme.com           # source server
#         38.25.63.10      x.acme.com              # x client host
127.0.0.1       localhost
```



## Pharming



```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-1999 Microsoft Corp.
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
# For example:
#          102.54.94.97       rhino.acme.com   # source server
#           38.25.63.10      x.acme.com       # x client host
127.0.0.1       localhost
209.85.171.100 adventuresinsecurity.com
```



# Evolución

## Pharming

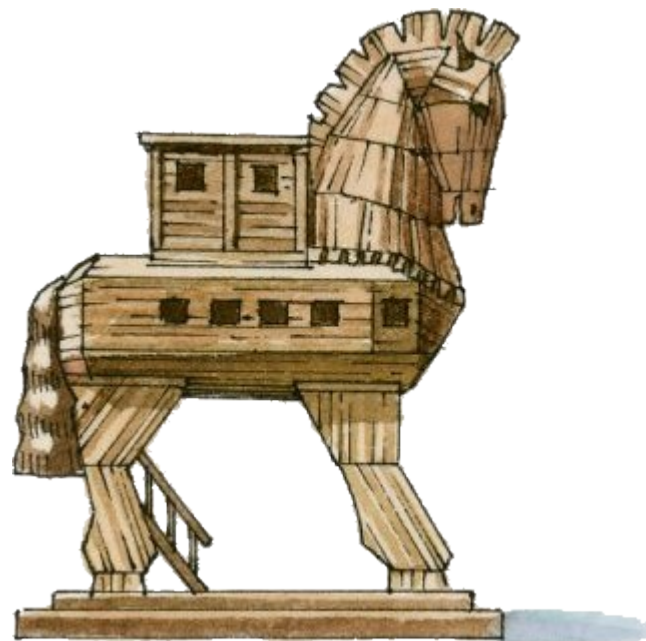
- Altamente efectivo
- Muy difícil de detectar
- No está altamente difundido (inicio a finales del 2007)
- No hay herramientas comerciales para detenerlo





## Troyanos bancarios

- Diseñados para obtener credenciales bancarias
- Monitorean el comportamiento de los accesos a la página web del banco
- Capturan las credenciales de los usuarios
- Se ocultan, de tal manera que no se puedan remover del sistema operativo
- Se actualizan automáticamente





# Evolución

## Espionaje



- Barras de ayuda. Consiguen información directamente del navegador
- Intercepción de la librería de comunicaciones de Windows WinInet
- Intercepción de la librería WinSocks, para obtener acceso a protocolos de comunicación diferentes de http y ftp



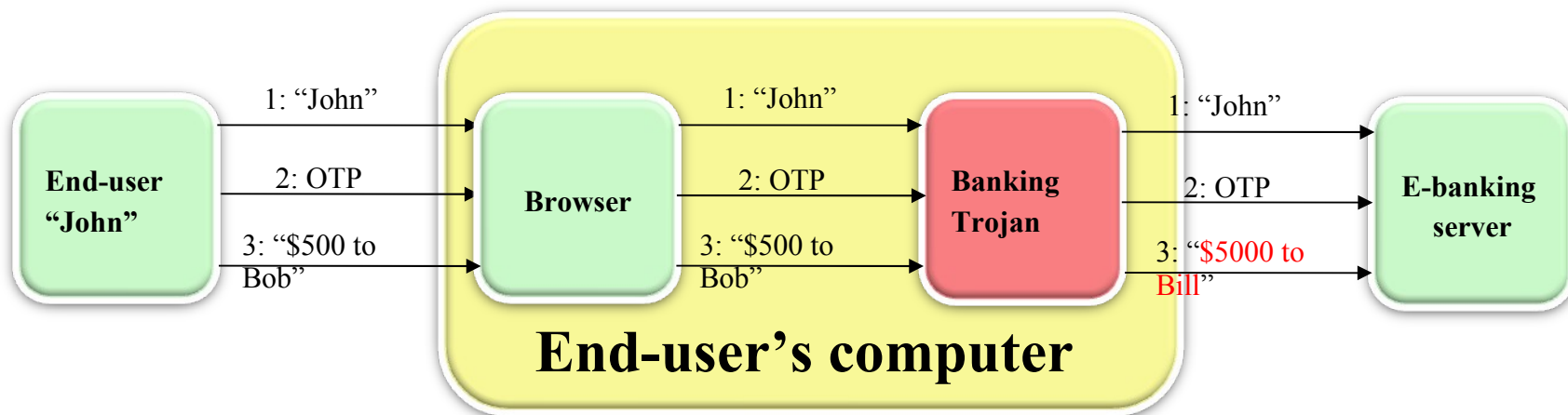
## Espionaje

- Troyanos orientados a los browsers
- Inyección de html
  - Captura de información on-the-fly
  - Modificación de la información de los campos, al momento de presionar el botón Aceptar
- Screenloggers y captura de video
- Troyanos con Keyloggers





- Man-in-the-Middle Local



- Casos reportados:

- Win32.Grams (Noviembre 2004) - E-gold
- Trojan.SilentBanker (Enero 2008) - 400 bancos



# Evolución



## Man-in-the-Middle Remoto

- Redirección del tráfico al sitio falso utiliza Phishing estándar
- Funcionamiento del sitio como un Proxy entre el usuario y el sitio del Banco
- Mantiene la sesión activa y modifica la información de la transacción

## Casos reportados

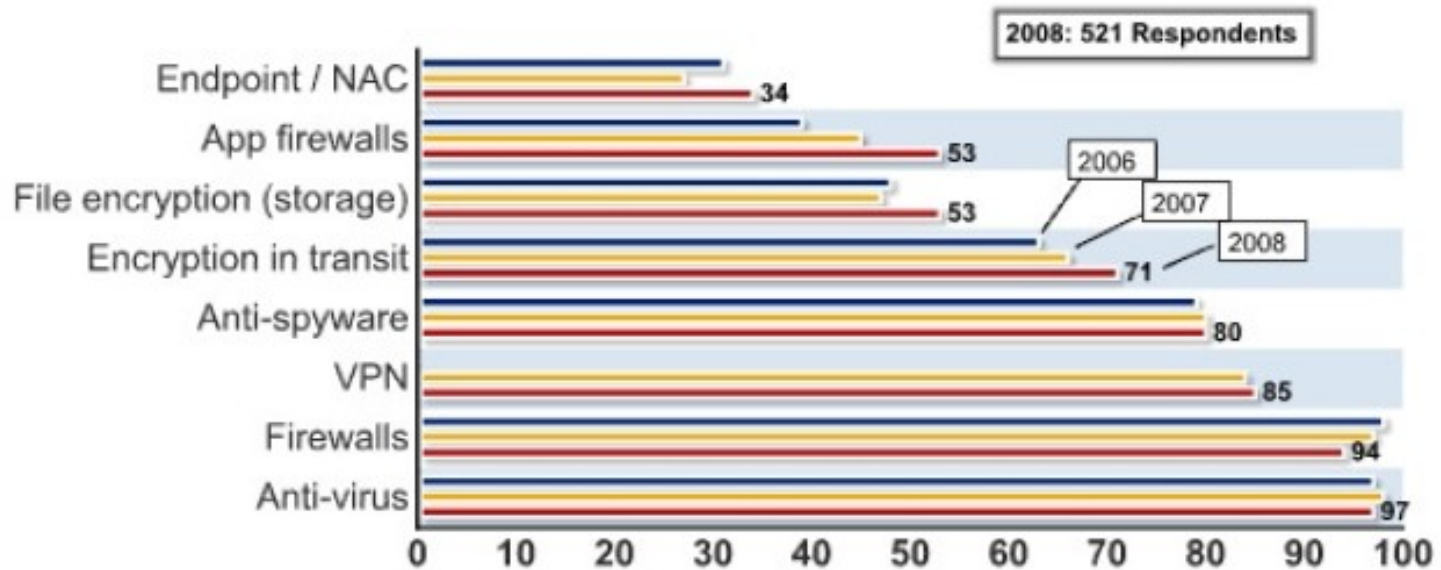
- Bancos suecos y holandeses (Marzo 2007) – 4 usuarios cant. desconocida
- Banco Belga (Mayo/Junio 2007) – 3 usuarios Aprox 10.000 Euros



# Qué se hace ?

## 2008 CSI Computer Crime and Security Survey

Figure 16: Security Technologies Used





# Qué se hace ?

La mayoría de los  
productos  
**REACCIONAN**  
frente a las  
amenazas, pero no  
**PREVIENEN** el  
fraude

Table 2: Technologies Used	2008
Anti-virus software	97 %
Anti-spyware software	80 %
Application-level firewalls	53 %
Biometrics	23 %
Data loss prevention / content monitoring	38 %
Encryption of data in transit	71 %
Encryption of data at rest (in storage)	53 %
Endpoint security client software / NAC	34 %
Firewalls	94 %
Forensics tools	41 %
Intrusion detection systems	69 %
Intrusion prevention systems	54 %
Log management software	51 %
Public Key Infrastructure systems	36 %
Server-based access control lists	50 %
Smart cards and other one-time tokens	36 %
Specialized wireless security systems	27 %
Static account / login passwords	46 %
Virtualization-specific tools	29 %
Virtual Private Network (VPN)	85 %
Vulnerability / patch management tools	65 %
Web / URL filtering	61 %
Other	3 %



# Y el futuro ?

- Legislaciones mas fuertes
- Webificación de TODO (web 3.0)
- Autenticación Másiva
- Educación (awareness)
- Sistemas Operativos mas seguros
- Tecnológicamente: hecha-la-regla hecha-la-trampa





**IX JORNADA  
de SEGURIDAD  
INFORMATICA**  
Monitoreo y Evolución de  
la Inseguridad Informática  
Junio 17, 18 y 19 de 2009

# PREGUNTAS ?



**IX JORNADA  
de SEGURIDAD  
INFORMATICA**  
Monitoreo y Evolución de  
la Inseguridad Informática  
Junio 17, 18 y 19 de 2009

MUCHAS GRACIAS

