¿Quién se ha comido mi dato?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio (Seguridad)

Introducción

- Satec. Vocación de servicio
- Los buenos
- Los malos
- ¿Que pasa mas alla de mi router?
- Lo que hemos aprendido
- ¿Apagamos los ordenadores?

SATEC. VOCACIÓN DE SERVICIO

¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC

Presentación de la unidad

- Estamos de 20 aniversario
- Experiencia en el sector de mas de 10 años en seguridad
- Independencia de fabricantes
- Soluciones que se integran con la infraestructura existente
- Continuidad de la solución

Presencia del Grupo SATEC

El Grupo SATEC tiene presencia en cinco países:

- España
- Portugal
- Marruecos
- Argelia
- Túnez

Y en 10 Comunidades Autónomas con sedes en:

- Madrid
- Barcelona
- Valencia
- Sevilla
- Bilbao
- Oviedo
- Las Palmas de Gran Canaria
- Vigo
- Toledo
- Valladolid

- El Grupo SATEC dispone de una empresa para soluciones específicas de Centros de Proceso de Datos/Hosting/Housing:

InterHost

LOS BUENOS

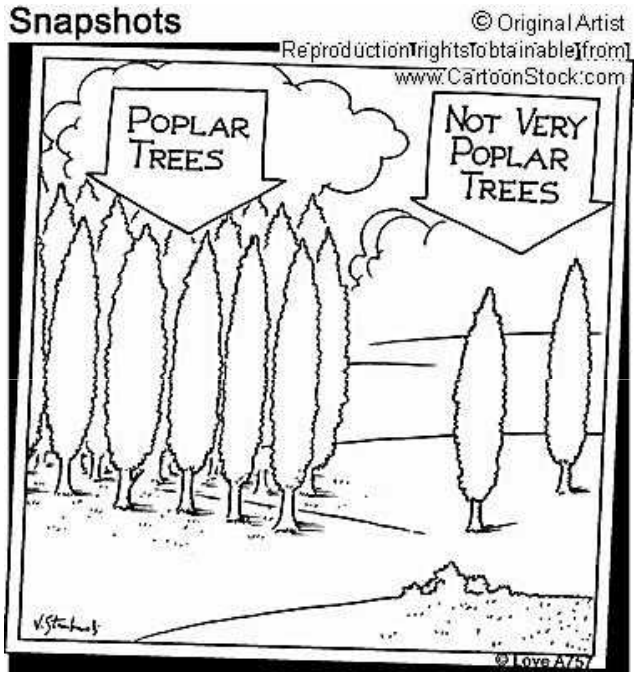
Luis Herreros Sánchez

Desarrollo de Negocio SATEC

Personal de seguridad

Seguridad aplicada

- Soluciones caras y poco populares
- El ROI es dudoso
  - Para que invertir, si no me pasa nada…
  - Normalmente se manifiestan vicios ocultos en la implantación.
- Iniciativas impulsadas desde la Dirección



Planteamientos que no bastan

- Existen medidas tecnológicas, pero…
  - ¿Cómo priorizar?
  - ¿Cuánto invertir?
  - ¿Cómo estar al día?
- También metodológicas, pero…
  - ¿Sabemos si son las adecuadas?
  - ¿Sabemos si se cumplen?
  - ¿Podemos medir su efectividad?
- ¿Lo estamos haciendo bien?
- ¿Podemos saberlo?

¿Qué es lo que falla?

¿Estamos a la altura de la tecnología?

¿Qué es lo que falla?

¿Sabemos si las medidas de seguridad funcionan?

¿Qué es lo que falla?

¿Son proporcionadas a lo que queremos proteger?

¿Qué es lo que falla?

¿Sabemos al menos si son las medidas adecuadas?

LOS MALOS

Evolución de los hackers

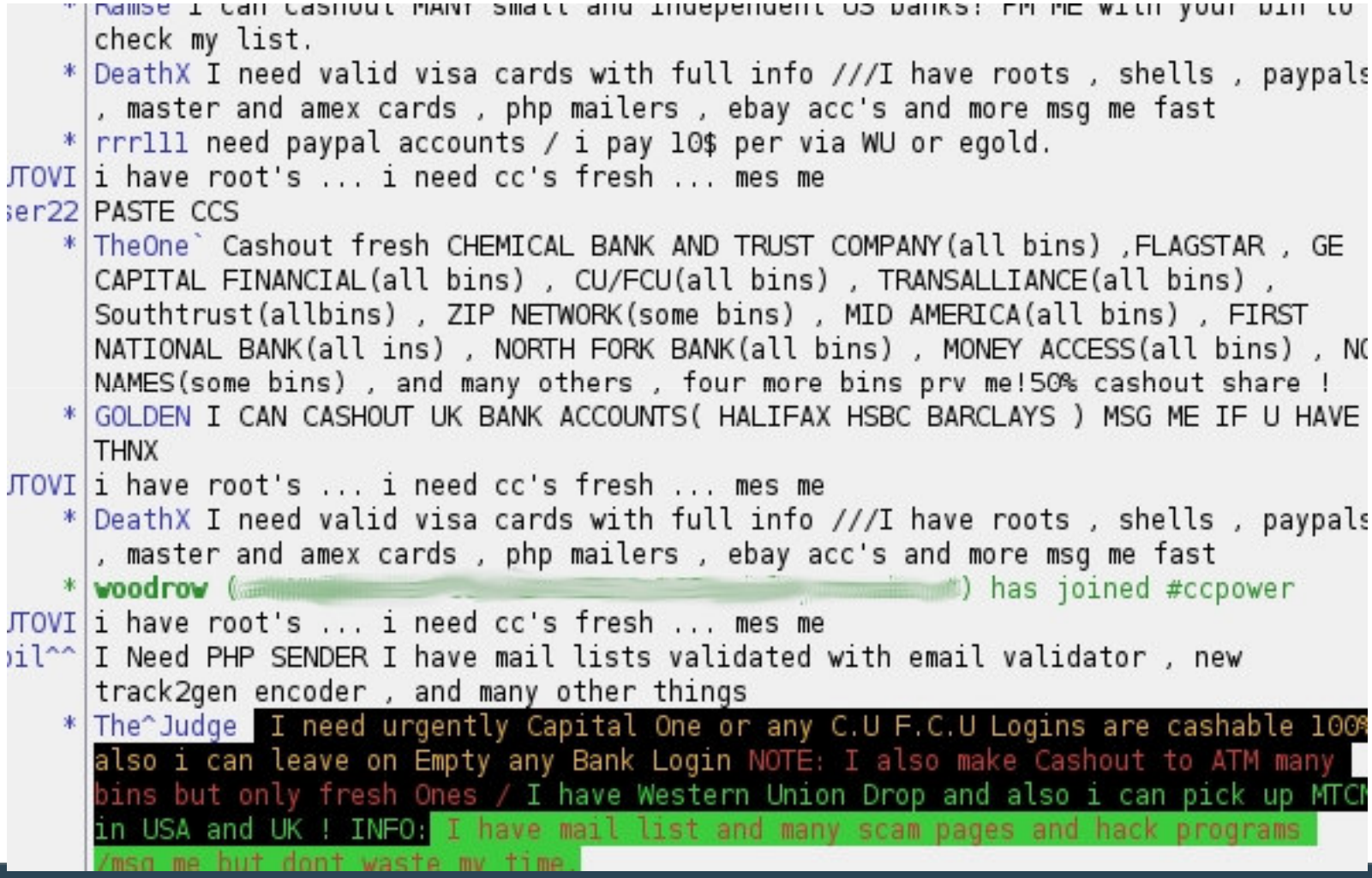
Motivación…

- Valerie McNiven, US Treasury advisor on cybercrime:

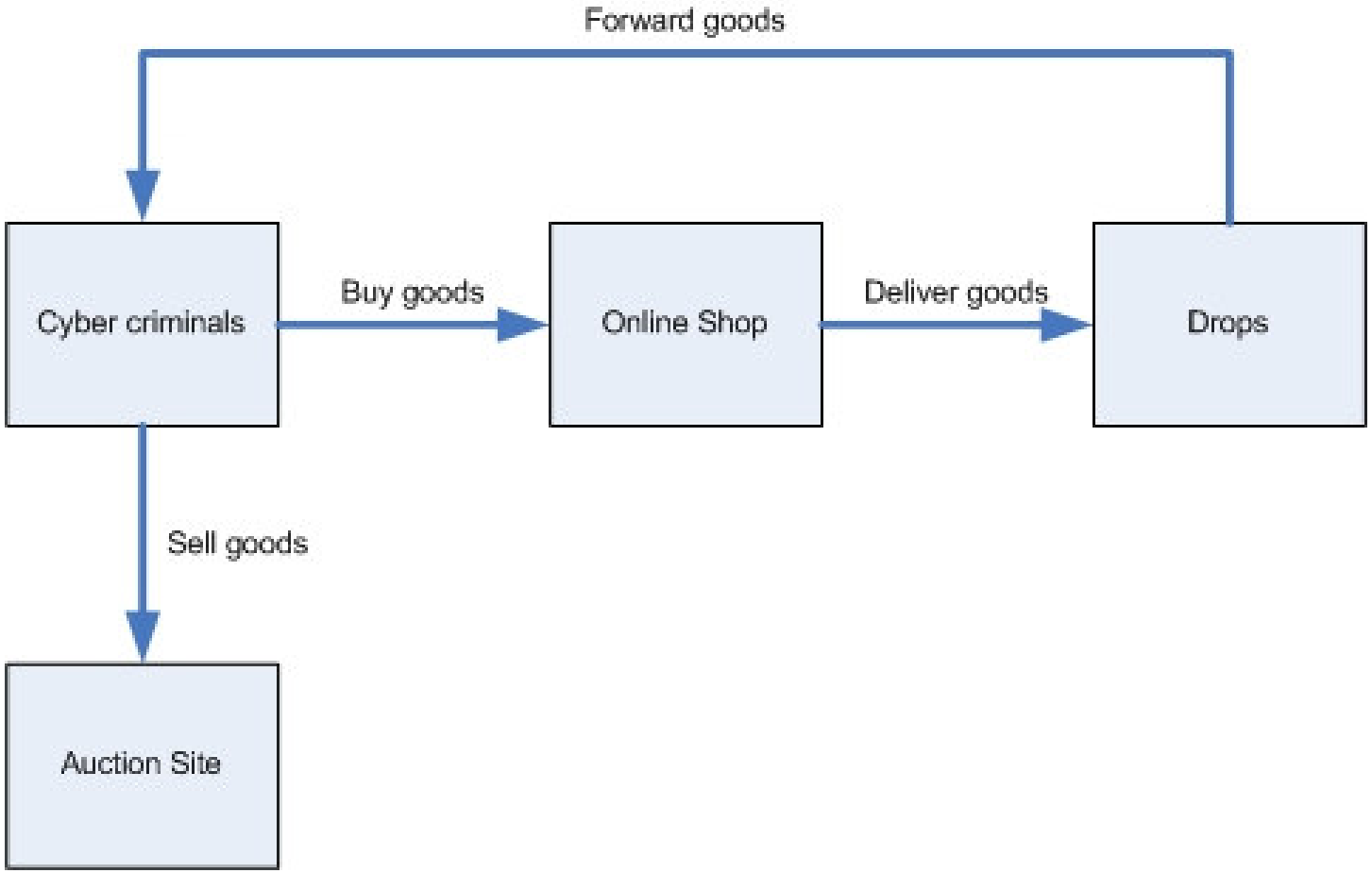
  "Last year was the first year that proceeds from cybercrime were greater than proceeds from the sales of illegal drugs, and that was, I believe, over $105 billion" [1]

[1] Reuters, **2005**

¿Dónde sacan los datos?



¿Cómo obtienen el dinero?



Costes vs Beneficios

- Costes
  - ✓ Comprar 40 CC validas: **$200**

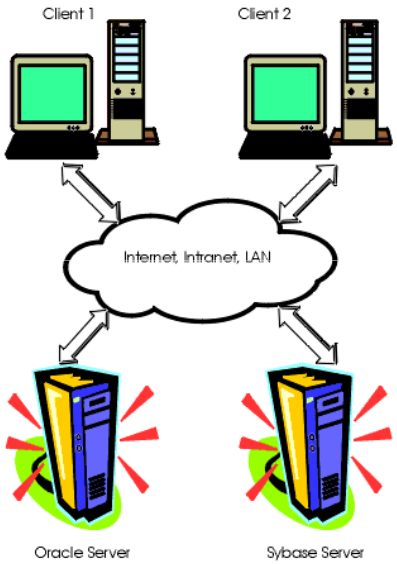
Profits

- ✓ Vender lo que compras en e-Bay: **$16,000 (**$400 por objeto)

- Coste mensual: **$200**
- Facturación mensual: **$16,000**
- Ganancias netas: **$15,800**

Punta de la Montana de Hielo/Iceberg

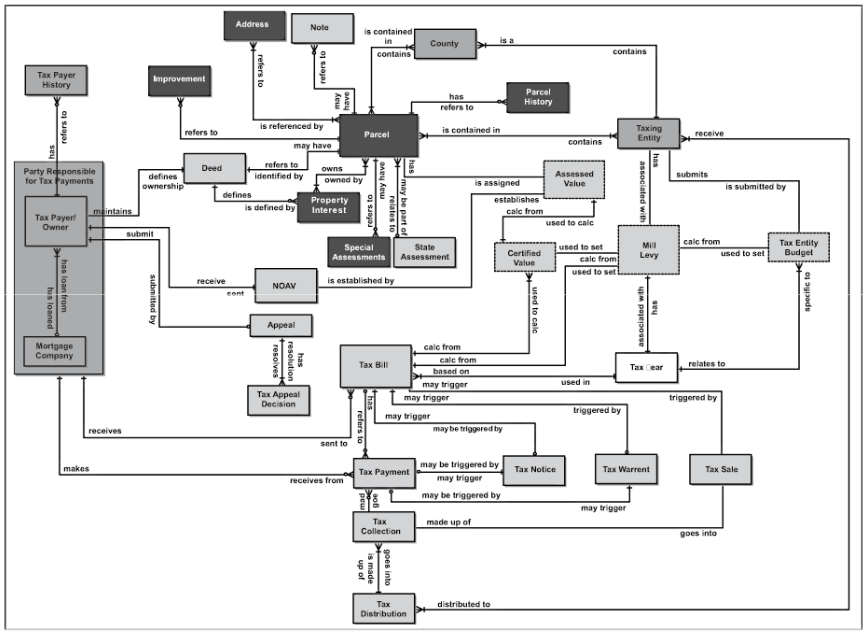
El modelo de 1999



- Orientado a la base de datos
- La información esta custodiada en los CPD
- Seguridad medieval

El modelo del 200…

- Los datos fluyen por la red
- Uso de dispositivos móviles
  - Portátiles
  - Teléfonos y PDA
  - Dispositivos USB
- Google



¿QUÉ PASA MAS ALLÁ DE MI ROUTER?

SQL Injection

- **Caso típico: Login usando Nick y password**

  - **Y, ¿cómo lo programo?**

```
SELECT * FROM users WHERE nick =
'$parametroNick' AND pass = '$parametroPass';
```

SQL Injection

- **Como no soy tonto, hago mis pruebas...**

Comprobación de validez:

```
SELECT * FROM users WHERE nick = admin AND pass = admin;
```

Comprobaciones de invalidez:

```
SELECT * FROM users WHERE nick = admin AND pass = inventado;
SELECT * FROM users WHERE nick = inventado AND pass = admin;
SELECT * FROM users WHERE nick = inventado AND pass = inventado;
```

SQL Injection

– ¿¿T

SELEC ...lequiera

AND pa

AND pas

$parame

$parame

Dando ...to de la tabla

¡¡PERO COMO ES POSIBLE!!

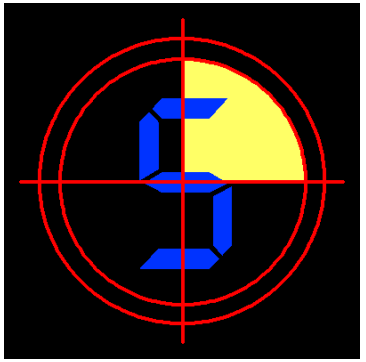
SQL Injection

- **Pero no solo se puede poner eso...**
  - **‘ OR ‘1’ = ‘1**  **Famosa cadena mágica**
  - **‘; DROP TABLE ‘users**
  - **‘; SELECT * FROM users WHERE pass LIKE '%**
  - **…**
- **Situación actual: técnica muy efectiva**

El eslabon mas debil

- 

Evolución de los ataques



El Phishing está cambiando

¿Qué es?

El hacker crea un sitio falso (similar a uno conocido) y obtiene datos confidenciales.

Nuevas tendencias

Pharming

Spear Phishing – ingeniería social

Ataques por errata – p.ej. : googkle.com

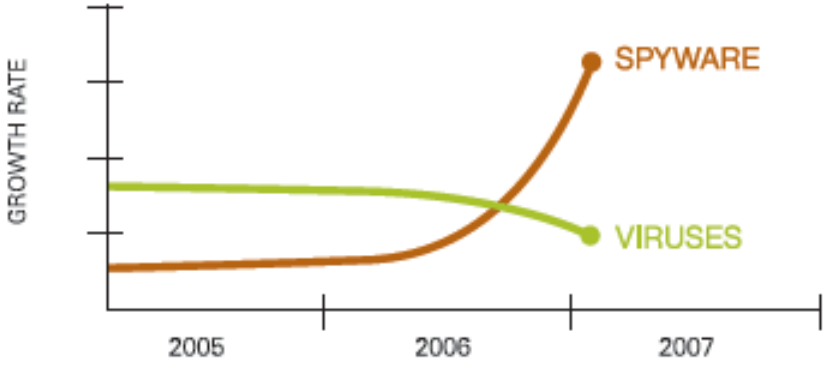
1/3 de los sitios de phishing alojan malware

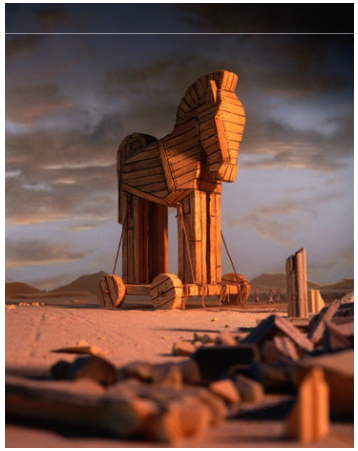
Tiempo medio en línea de un sitio de phishing es de 3,6 días

Fuente : Anti-Phishing Working Group

El Malware prolifera

- 150.000 tipos diferentes de spyware
- El 7% de los PCs corporativos están contaminados con un troyano
- Registradores de pulsaciones del teclado (keyloggers): se han multiplicado por 20 en 5 años, evolución actual: capturadores de pantalla
- Gran crecimiento de rootkits (herramientas diseñadas para esconder otros códigos más maliciosos)





Las redes zombis se están multiplicando

- El hacker toma control de forma remota de un PC gracias a un código malicioso durmiente que no tiene acción inmediata. El hacker puede entonces comenzar un ataque remoto gracias a ese código.

- El PC contaminado se convierte realmente en un zombi, siguiendo las órdenes del hacker.

- 200.000 nuevos PCs contaminados por día

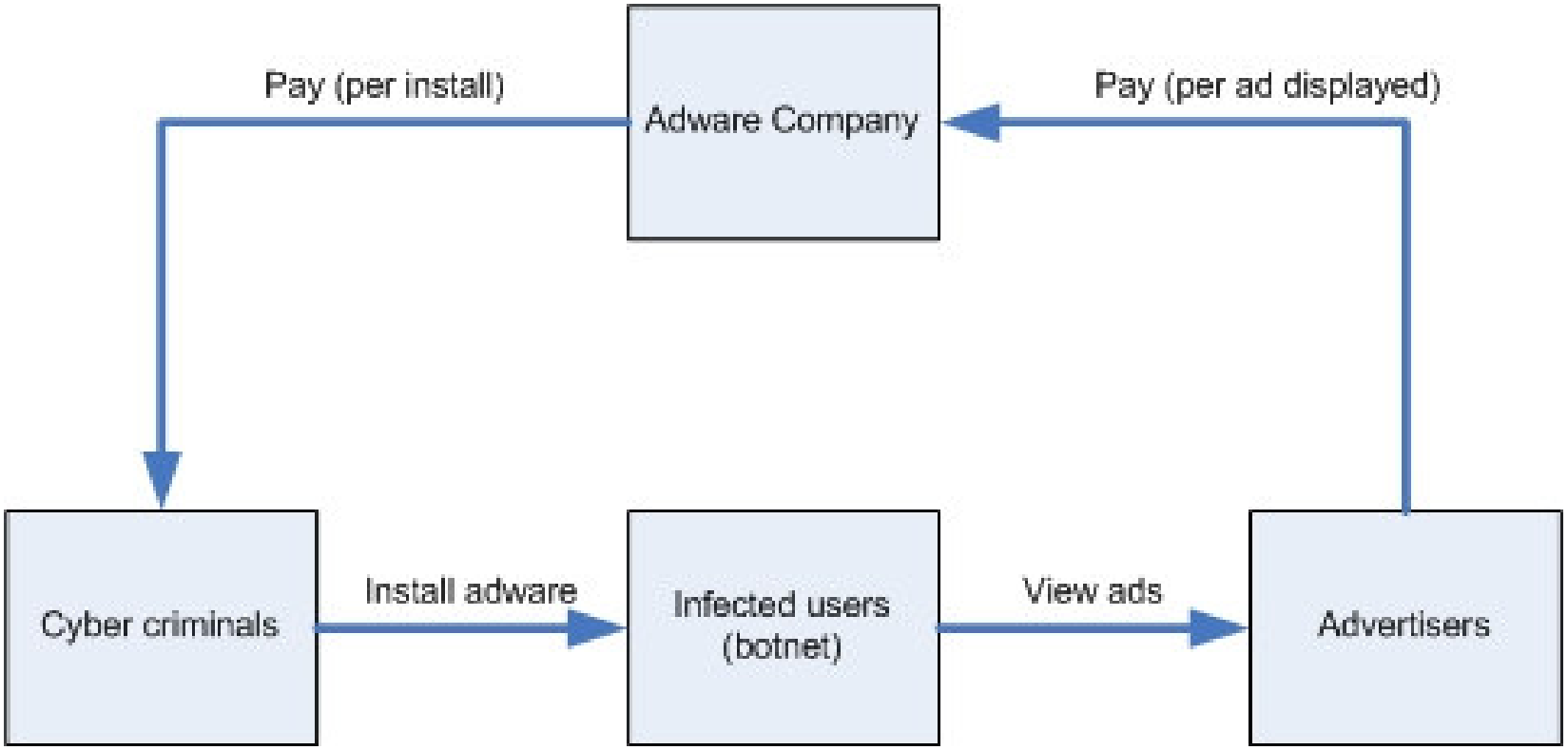
- Vida media de un zombi : menos de 1 mes (2006)

- Usos : denegación de servicios, ciber-extorsión, phishing, spam, etc.

La red Storm

- **La red bot más importante del mundo**
  - –1.000 PCs contaminados se alquilaban por $220 en Alemania
  - –1.000 PCs contaminados en USA $110
  - – Se alquilaban por hora, con soporte telefónico disponible
- **Auto-expansivo:** e-mails para reclutar y spam tradicional
- **Coordinado**: Sincroniza spam de correo con sitios web de inicio
- **Peer-to-Peer**: Usa redes P2P y flujo rápido
- **Reutilizable**: Spam, Phishing, DDoS, Blog Spam
- **Auto-defensivo**: lanza un DDoS a aquellos que tratan de localizarlos

Un caso de éxito…

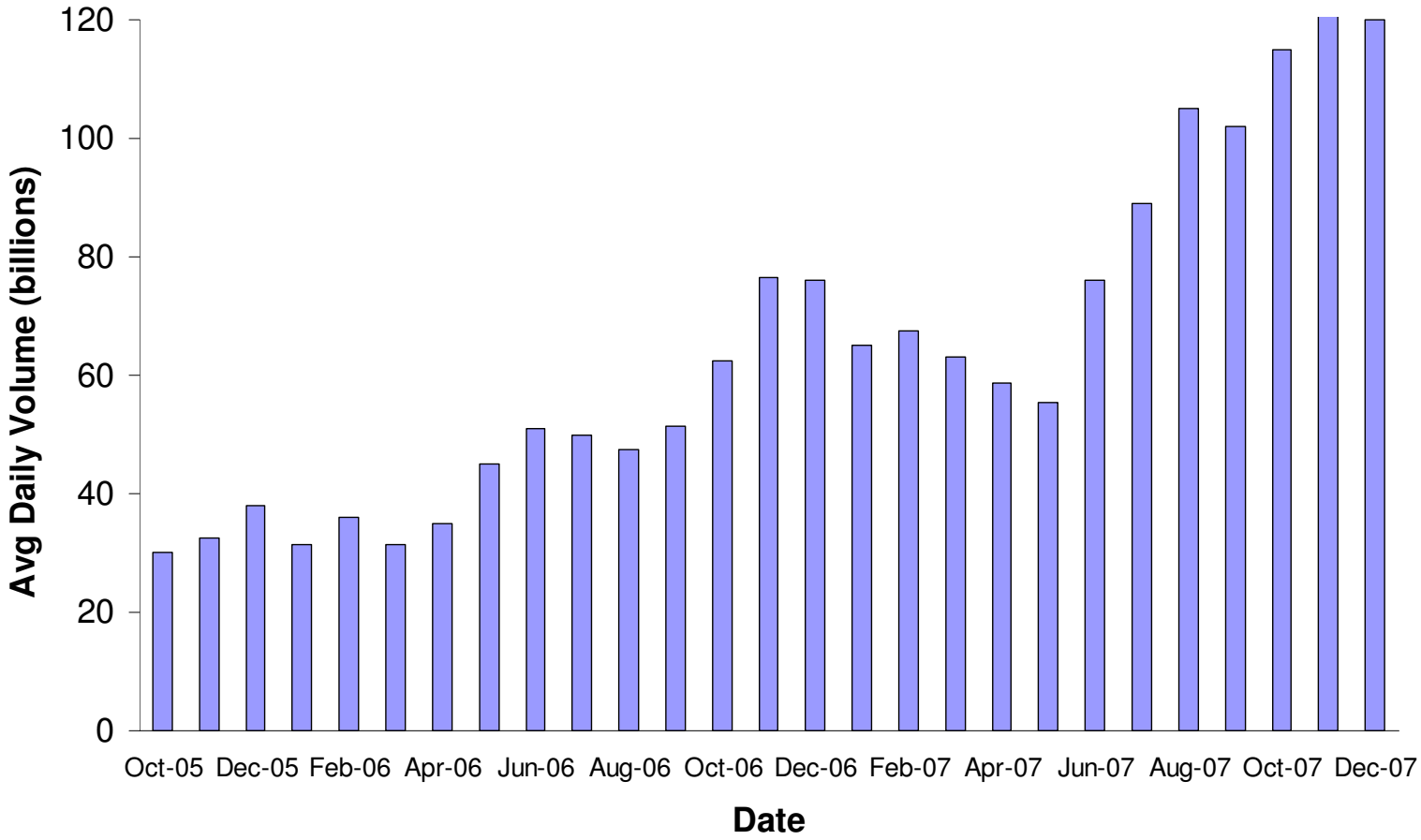


Los números…

- Costes de crear una red de zombies:
  - ✓ Maquina de control: **$15**
  - ✓ Numero de CC robado para facturar **$2**
  - ✓ Codigo fuente del bot: **$2**
  - ✓ Conseguir que no sea detectable por los antivirus durante 3 dias **$100**
  - ✓ Lista de spam fresca: **$8**
  - ✓ Grupo de maquinas relay para realizar la compra masiva: **$30**
- *Coste total*: **$157** (una vez)
- *Beneficio total*: 0.4 x 5000 x 8 = **$16,000** (mensual)
- *Ganancias netas*: **$15,843** (Primer mes)

¡El spam continúa creciendo!

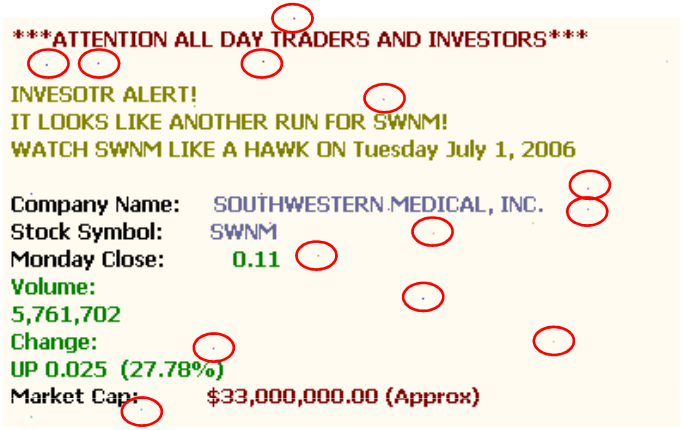
¡x4 en 2 años!



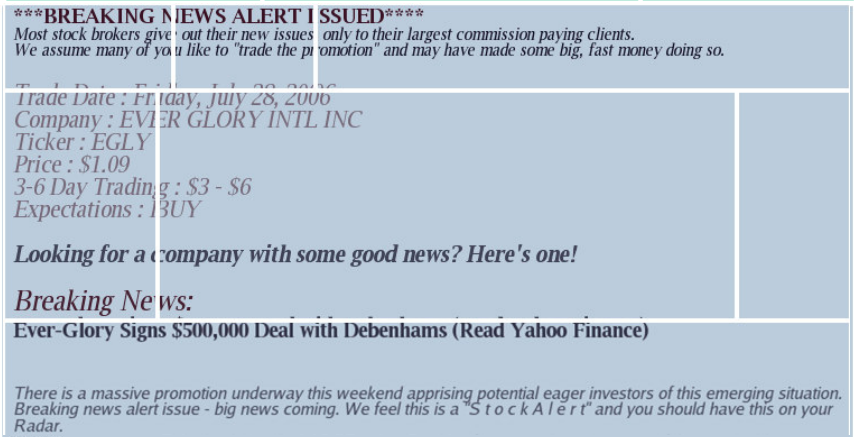
Spam de imágenes

Gran « innovación » de 2006 y principios de 2007

1. “Puntos Polca”



2. Cortes de imágenes



Otras técnicas de 2007

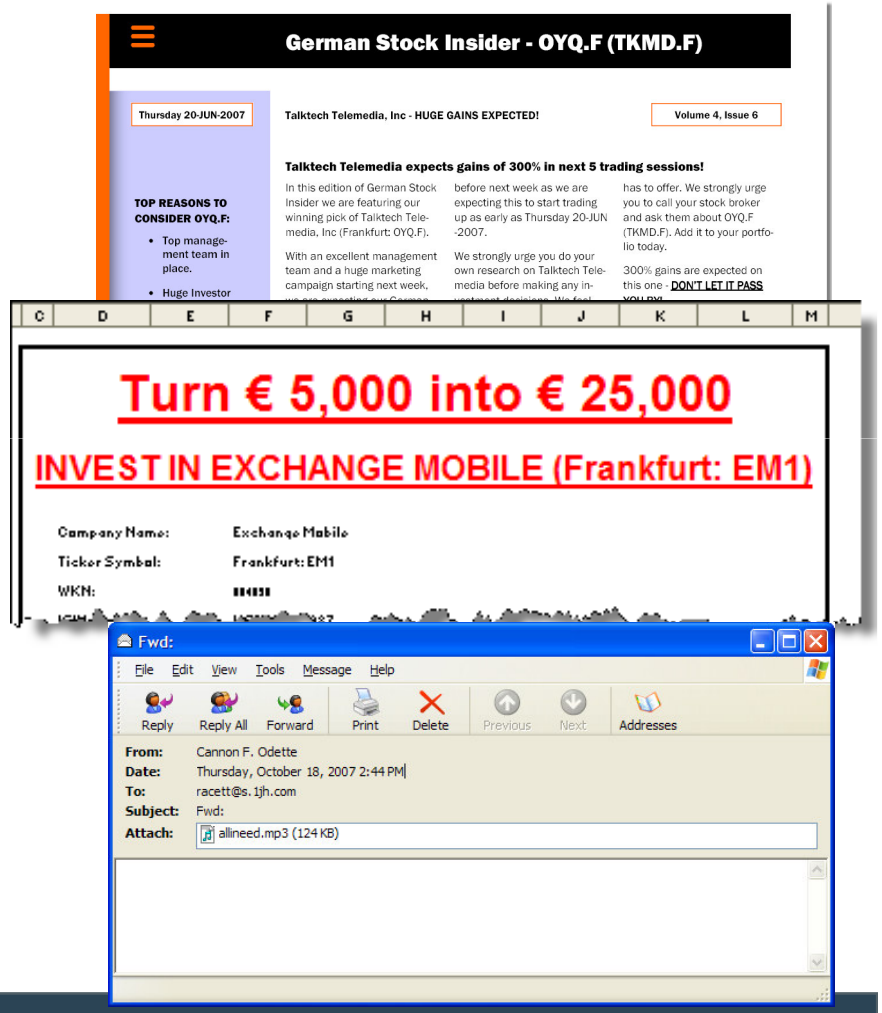
20 tipos diferentes de archivos adjuntos

- Los ataques en 2007 fueron breves, pero más frecuentes y, cada uno de ellos, con diferentes técnicas.

- Se utilizaron más de 20 tipos diferentes de archivos adjuntos: PDF, Excel, MP3, etc.

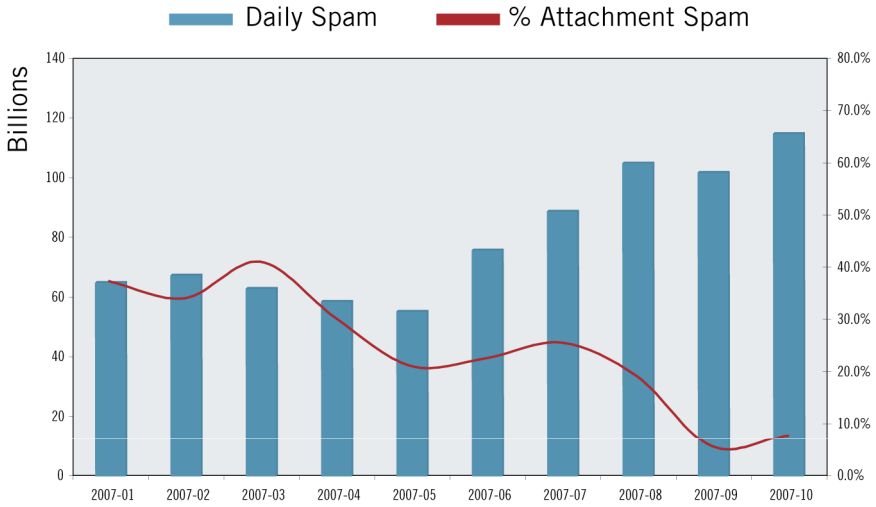
Protección necesaria

- Herramientas de reputación que puedan bloquear proactivamente la mayoría del spam al identificar los bots que están enviando spam.
- Poderoso motor Anti-Spam: capaz de emitir reglas basadas en el tipo del fichero, contenido del archivo, tamaño del mensaje y otra información para capturar el spam restante. De esta forma, no es necesario bloquear todos los archivos PDFs o Excel.



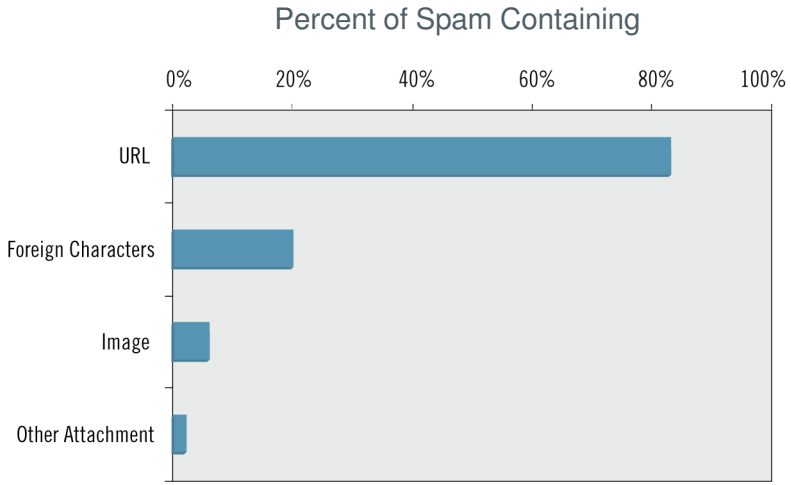
La nueva técnica: URL spam

De las imágenes a los enlaces web



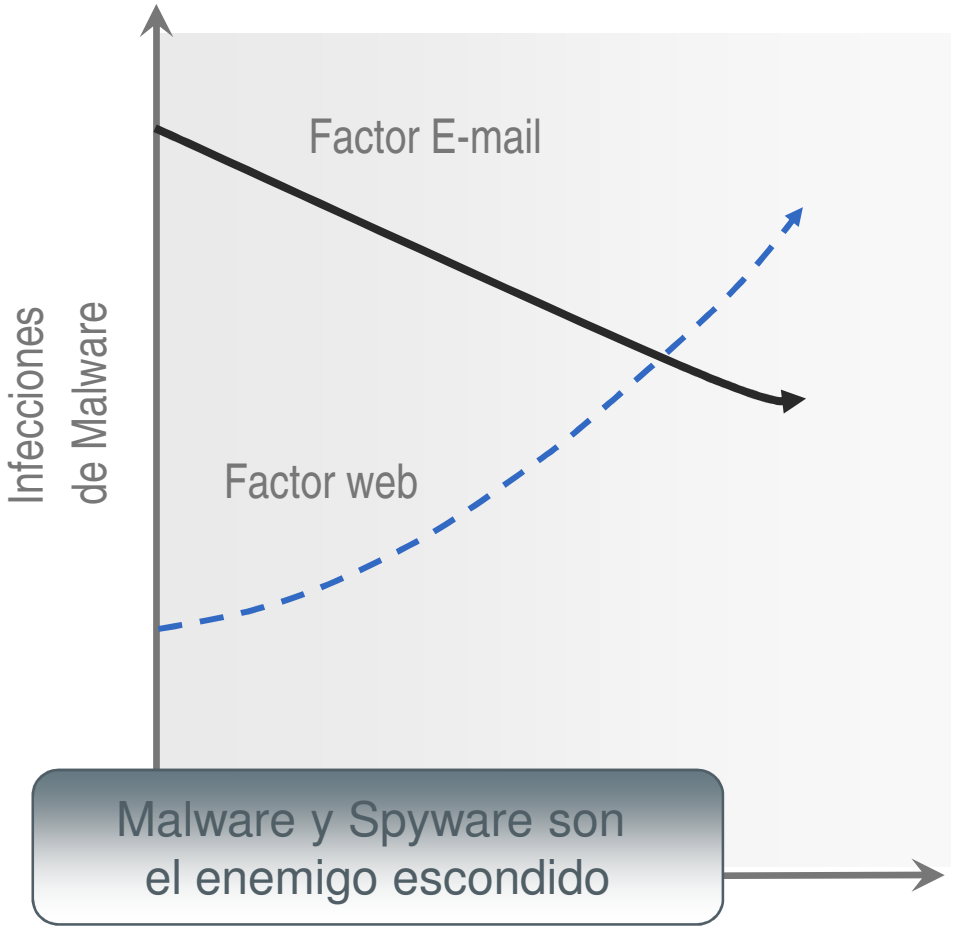
El URL spam continúa creciendo
(+ 253% en 2007 vs 2006)

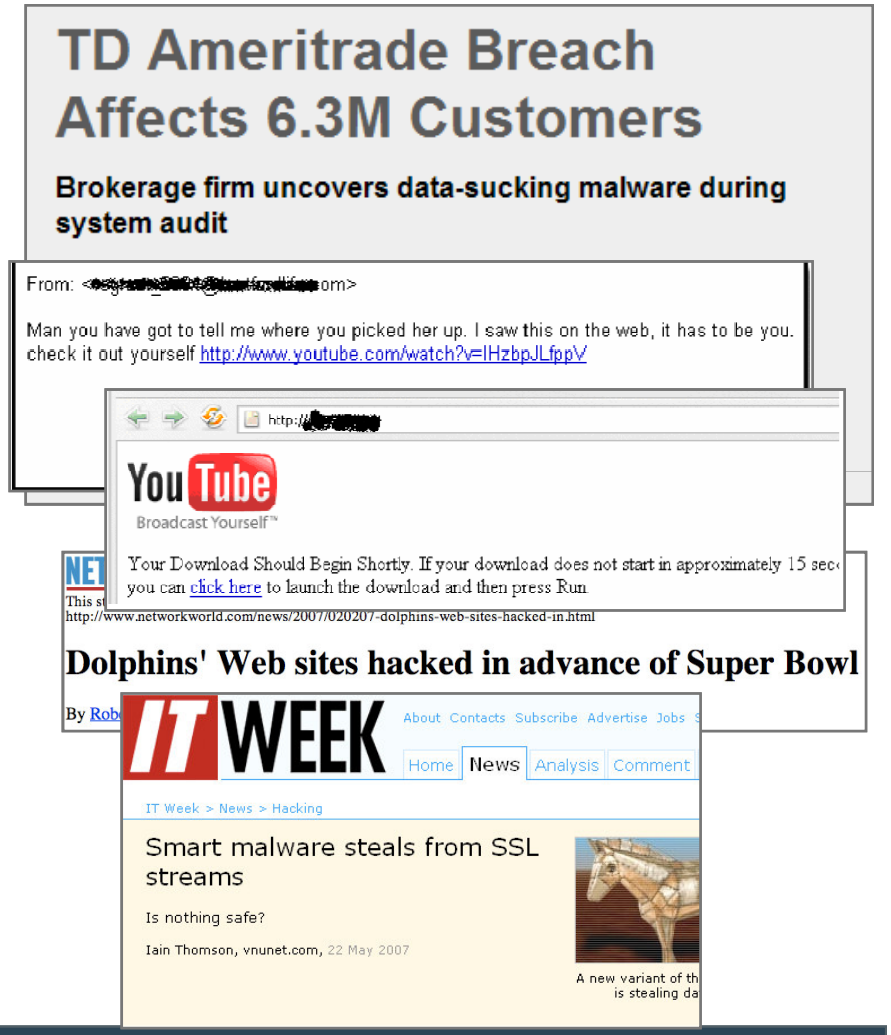
El spam continúa creciendo, pero el spam de archivos adjuntos se reduce



Factores de amenazas de malware

Cambiando del e-mail a la web





Técnicas de infección web

- Un malware insertado en una « buena » aplicación
- Hacer clic en un pop up
- Descarga automática, sin ninguna acción por parte del usuario, y sin que el usuario se dé cuenta en absoluto

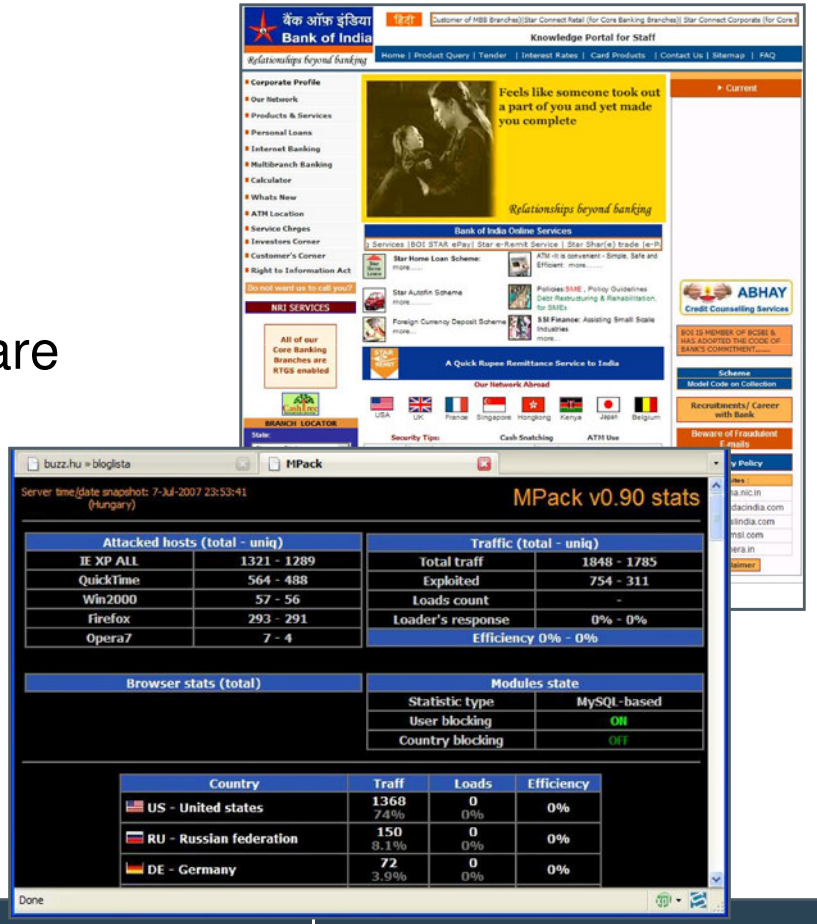
70% de las infecciones basadas en Web se encontraron en sitios web 'legítimos'

1 de cada 10 páginas web están infectadas con código malicioso

(Investigación de Google, mayo de 2007)

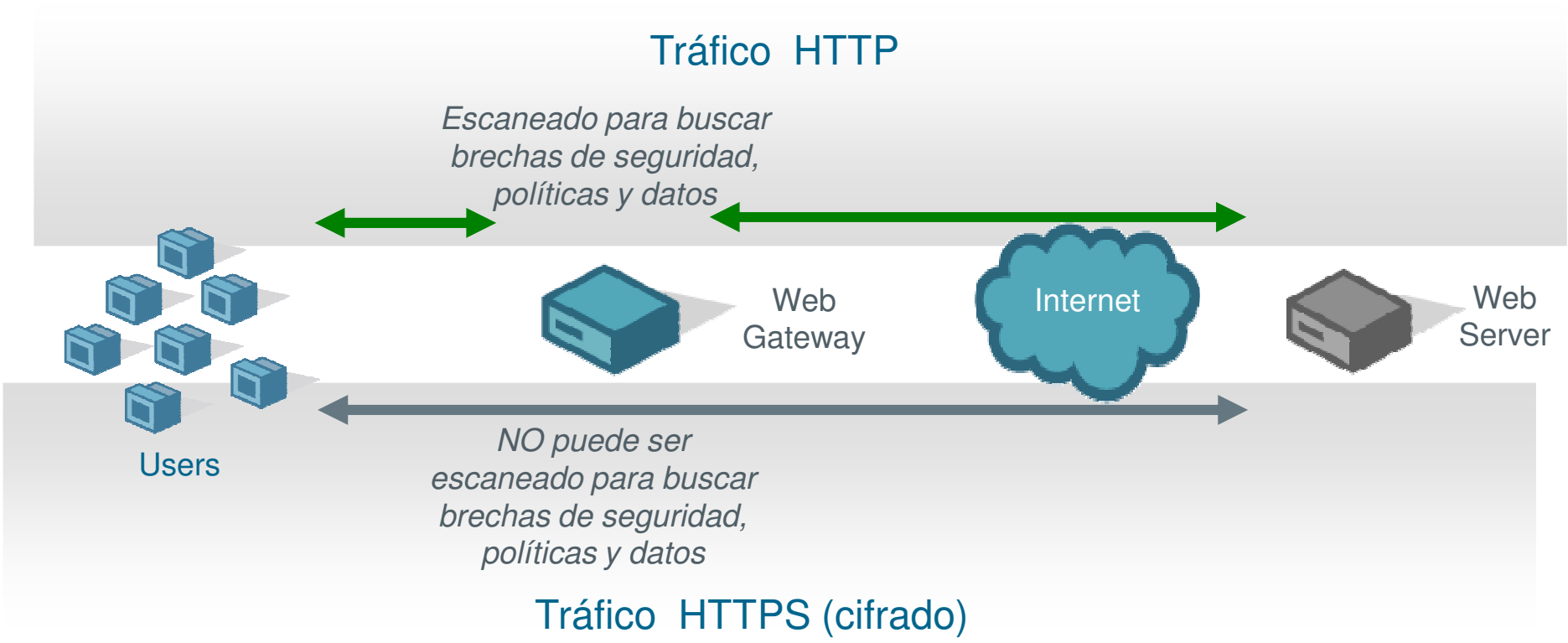
Sitios legítimos hackeados

- Sitios web legítimos se convierten en puntos de distribución
  - –Ataques iFrame
  - –Miami Dolphins, Bank of India
  - –Hack masivo Mpack
- Los usuarios introducen el malware dentro de la red



HTTPS

Un punto ciego para las empresas



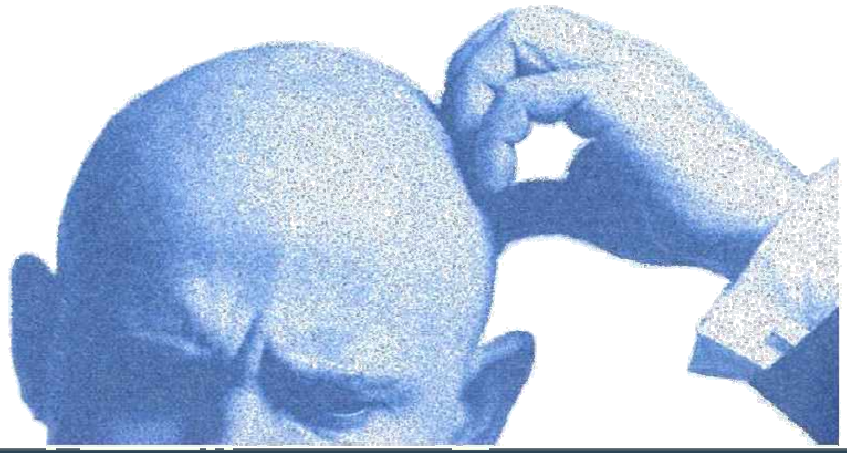
LO QUE HEMOS APRENDIDO

Seguridad “de película”

- Es una guerra asimétrica:
  - El atacante sabe qué va a atacar: un objetivo.
  - El defensor no: debe defender todo.
  - El atacante sabe cómo va a atacar: un método.
  - El defensor no: debe defender contra todo.
- “Movie plot threat” (Bruce Schneier).
  - Tenemos ejemplos en la lucha contra el terrorismo.
  - No importa cómo elija concentrar mis esfuerzos, el ataque vendrá de otra forma, y en otro sitio.
  - En último término ¿quién dicta mi política de seguridad?

¿Cuál es la solución?

- Necesitamos:
  - Gestionar el riesgo.
  - Medidas adecuadas: efectivas y proporcionadas.
  - Control sobre su funcionamiento y efectividad.
  - Reevaluar la situación continuamente.
- Y recordemos:
  - Justificar las inversiones.
  - Medir los resultados.
  - Calibrar el impacto político.
- Gestionar la seguridad.



Predicciones para 2008

- El año del “Malware Social”
  - Las amenazas utilizarán cada vez más los sitios colaborativos y serán adaptativas e inteligentes
  - Más ingeniería social, se aprovecharán del usuario final para saltarse los controles
- El volumen de spam continuará creciendo sin límite
  - Los filtros deben aumentar sus tasas de captura
  - Una consolidación de los fabricantes resultaría eficaz
- Continuará el uso de ataques combinados
- Las defensas deben cambiar
  - De sistemas basados en firmas a sistemas de reputación

¿APAGAMOS LOS ORDENADORES?

Calidad del código fuente

- Primamos mas el cuándo, que el cómo
  - HIPAA
- Si el esfuerzo es titanico…
  - Firewalls de nivel 7
    - Pero con la ingenieria adecuada
    - Evitar el efecto IDS

Ejemplo de madurez creciente: auditorías

Análisis de riesgos
Aporta el concepto de impacto
Aporta criterios organizativos
Es la base para un plan de continuidad
Nos permite priorizar y asignar recursos
Se sigue limitando a una “foto” estática

Revisión in situ de sistemas
Analiza riesgo real y potencial
Se limita a la visión interna

Test de intrusión (hacking ético)
Aporta la visión externa
No contempla riesgo potencial

Otro ejemplo: planificación

Política de seguridad
Orientada a objetivos
Define roles y responsabilidades
Define métricas de cumplimiento
Contempla su propia evolución
Planificación también proactiva

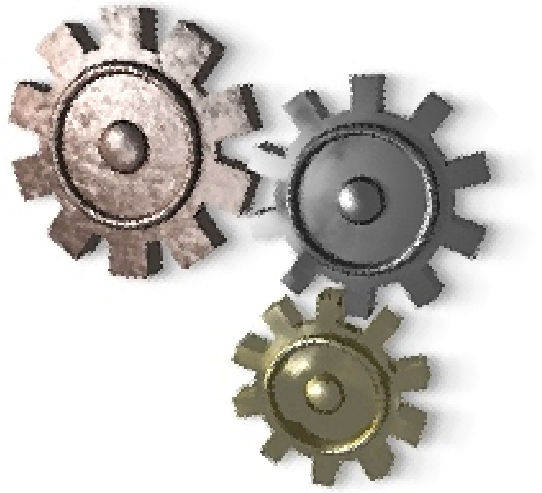
Planes de contingencia
Planificación sólo reactiva

Procedimientos ad-hoc
No hay planificación

Podemos unir ambos enfoques

El ciclo de mejora continua

- Conocido como ciclo PDCA o de Deming/Shewart.
- Aplicado en gestión de calidad.
- Pasos:
  - Plan: determinar qué hay que hacer.
  - Do: ¡hacerlo!
  - Check: verificar los resultados de la acción.
  - Act: implantar correcciones.
- La seguridad como ciclo.
  - Es un proceso (mientras lo sigues, estás más seguro).
  - No es un producto (no hay un fin – nunca has llegado).



Sistemas de gestión de seguridad

- Sistema de Gestión de Seguridad de la Información
  - Es un plan de mejora continua.
  - Tiene un alcance definido a la medida de la organización.
  - Utiliza análisis de riesgos y métricas de seguimiento.
  - Está vivo.
  - Se puede basar en estándares.
  - Se puede certificar.

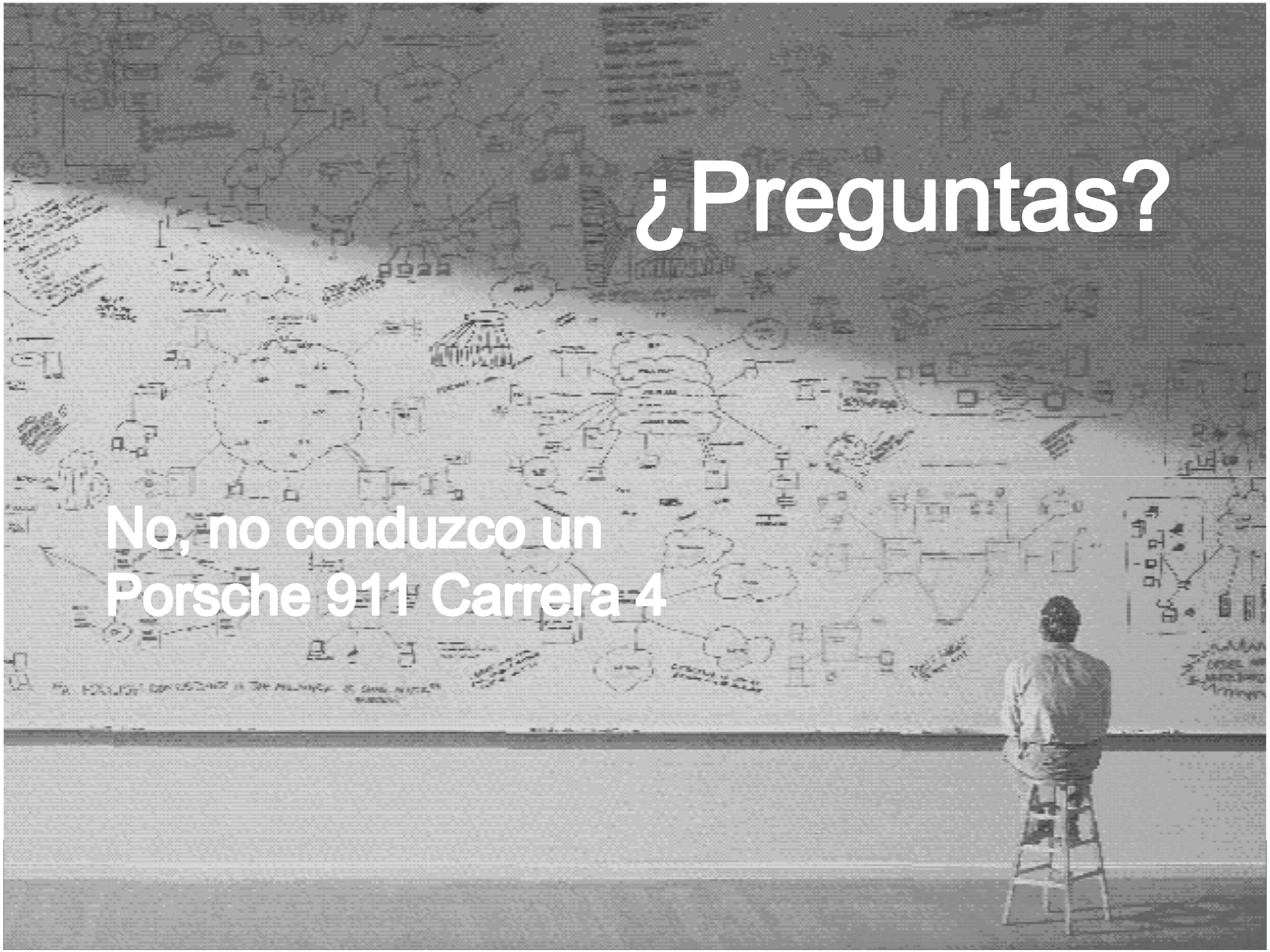
- Cualquier sistema de gestión es mejor que nada.

Tres ideas

- Las organizaciones primero adquieren productos, luego implantan procesos y finalmente forman personas.
- *Prueba al revés.*

- Más seguridad de la necesaria es derroche.
  Menos, es irresponsabilidad.
  Si no sabes cuánto debes gastar…
- *…tal vez la mejor inversión sea averiguarlo.*

- Mejor que prepararse para un riesgo concreto es estar dispuesto para lo imprevisto.
- *Menos seguridad en todo*
  es mejor que mucha en sólo algunas cosas.


¿Preguntas?
No, no conduzco un
Porsche 911 Carrera 4

Muchas Gracias

Luis Herreros Sánchez

lhsanchez@satec.es