



¿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

¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



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

¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



LOS BUENOS

¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



Personal de seguridad



¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

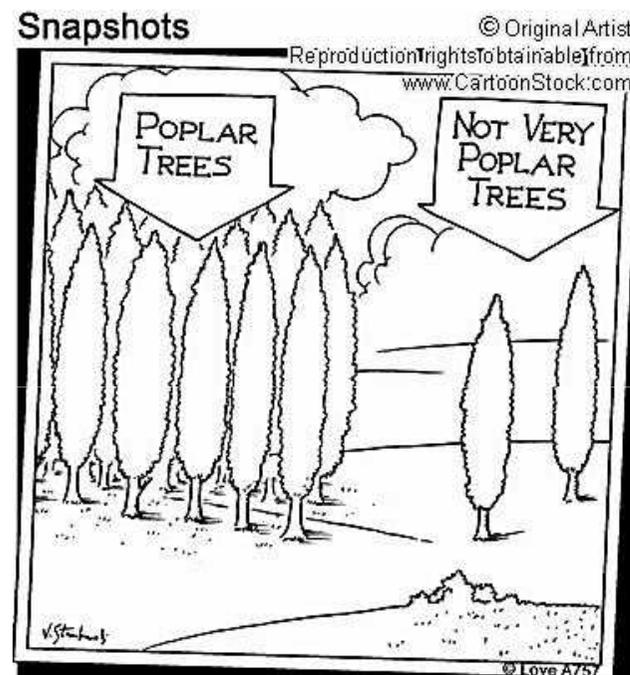
Desarrollo de Negocio SATEC

6



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



¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



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?

¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



¿Qué es lo que falla?



¿Sabemos si las medidas de seguridad funcionan?

¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



¿Qué es lo que falla?



¿Son proporcionadas a lo que queremos proteger?

¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



¿Qué es lo que falla?



¿Sabemos al menos si son las medidas adecuadas?

¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



LOS MALOS

¿Quién se ha comido mis datos?

Una parada para pensar...

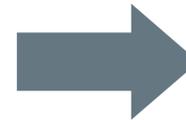
Luis Herreros Sánchez

Desarrollo de Negocio SATEC

13



Evolución de los hackers



¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



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?

```
* Rise I can cashout MANY small and independent US banks! PM ME with your bin to
check my list.
* DeathX I need valid visa cards with full info ///I have roots , shells , paypals
, master and amex cards , php mailers , ebay acc's and more msg me fast
* rrrlll need paypal accounts / i pay 10$ per via WU or egold.
JTOVI i have root's ... i need cc's fresh ... mes me
ser22 PASTE CCS
* TheOne` Cashout fresh CHEMICAL BANK AND TRUST COMPANY(all bins) ,FLAGSTAR , GE
CAPITAL FINANCIAL(all bins) , CU/FCU(all bins) , TRANSALLIANCE(all bins) ,
Southtrust(allbins) , ZIP NETWORK(some bins) , MID AMERICA(all bins) , FIRST
NATIONAL BANK(all ins) , NORTH FORK BANK(all bins) , MONEY ACCESS(all bins) , NC
NAMES(some bins) , and many others , four more bins prv me!50% cashout share !
* GOLDEN I CAN CASHOUT UK BANK ACCOUNTS( HALIFAX HSBC BARCLAYS ) MSG ME IF U HAVE
THNX
JTOVI i have root's ... i need cc's fresh ... mes me
* DeathX I need valid visa cards with full info ///I have roots , shells , paypals
, master and amex cards , php mailers , ebay acc's and more msg me fast
* woodrow ( [REDACTED] ) has joined #ccpower
JTOVI i have root's ... i need cc's fresh ... mes me
oil^^ I Need PHP SENDER I have mail lists validated with email validator , new
track2gen encoder , and many other things
* The^Judge I need urgently Capital One or any C.U F.C.U Logins are cashable 100%
also i can leave on Empty any Bank Login NOTE: I also make Cashout to ATM many
bins but only fresh Ones / I have Western Union Drop and also i can pick up MTCN
in USA and UK ! INFO: I have mail list and many scam pages and hack programs
/msg me but dont waste my time
```

¿Quién se ha comido mis datos?

Luis Herreros Sánchez

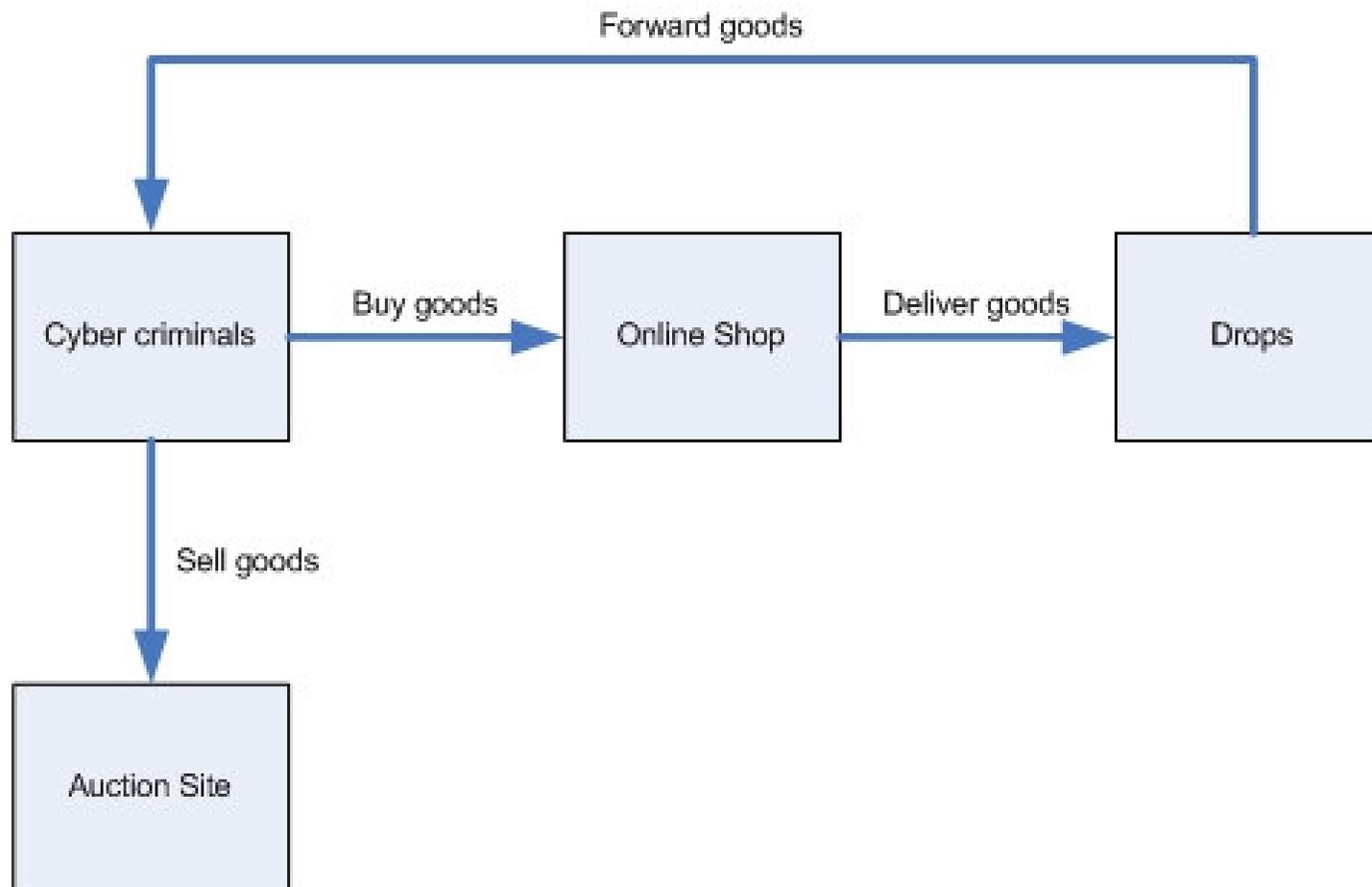
16

Una parada para pensar...

Desarrollo de Negocio SATEC



¿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 Montaña de Hielo/Iceberg



Que es lo que esta
derritiendose abajo
de la montaña...

¿Quién se ha comido mis datos?

Una parada para pensar...

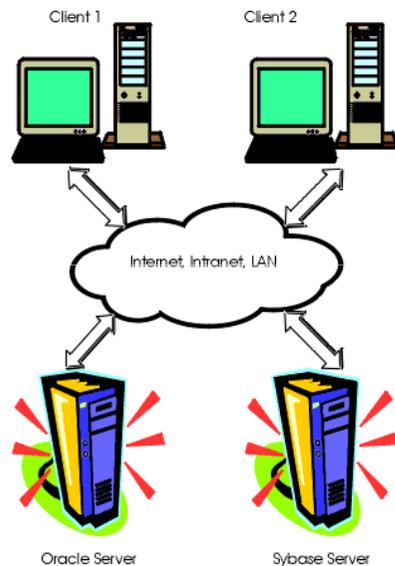
Luis Herreros Sánchez

Desarrollo de Negocio SATEC

19



El modelo de 1999



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

¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



¿QUÉ PASA MAS ALLÁ DE MI ROUTER?

¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC

22



SQL Injection

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



Nombre de usuario:

Contraseña:

Recordarme en este equipo.

– 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;
```

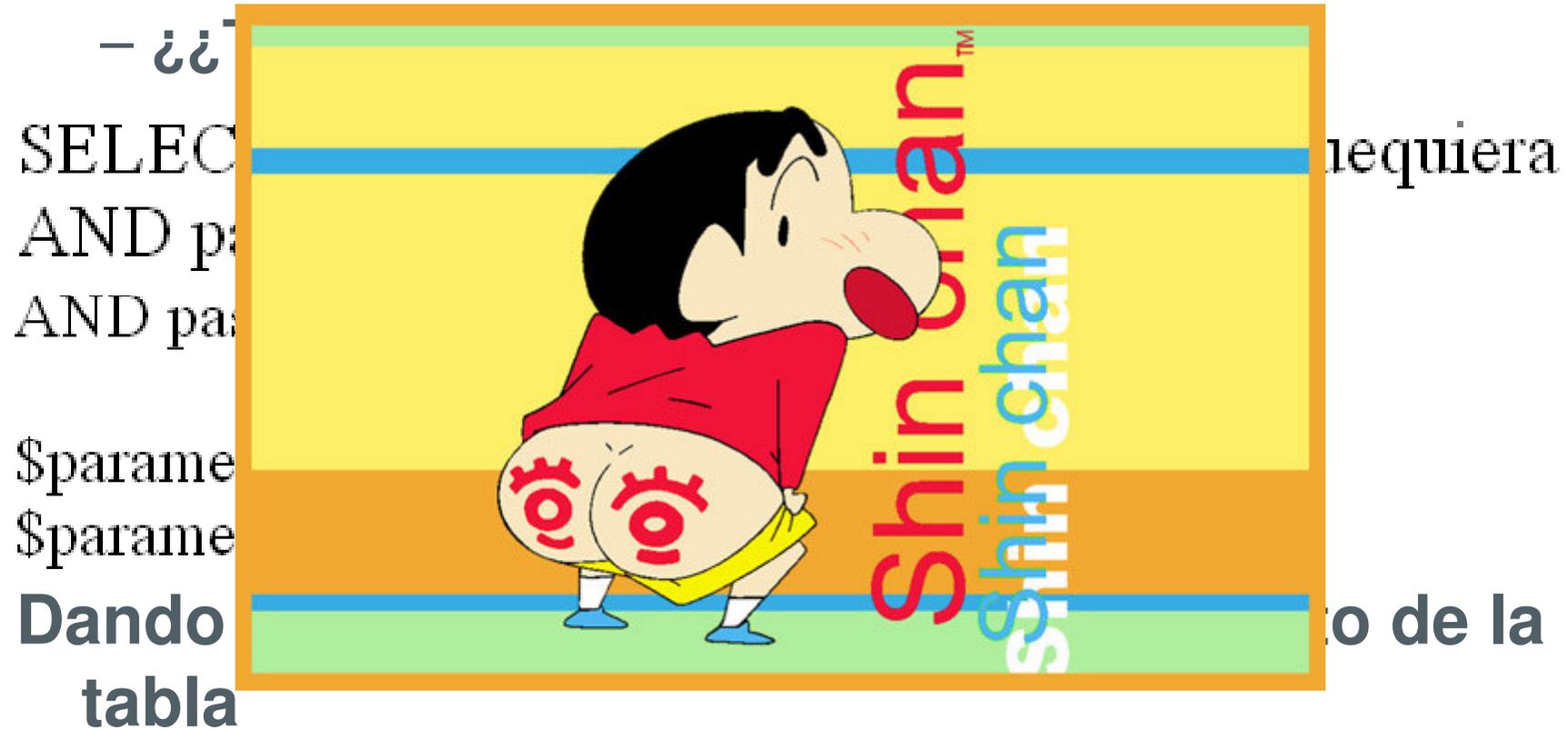
Comprobaciones de invalidez:

```
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



¡¡PERO COMO ES POSIBLE!!

¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC

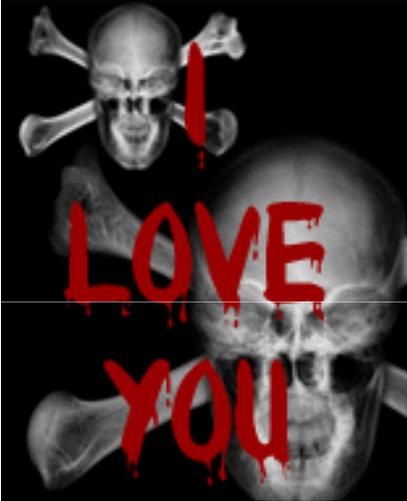


SQL Injection

- 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

Evolución de los ataques



¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



El Phishing está cambiando

¿Qué es?

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

Nuevas tendencias

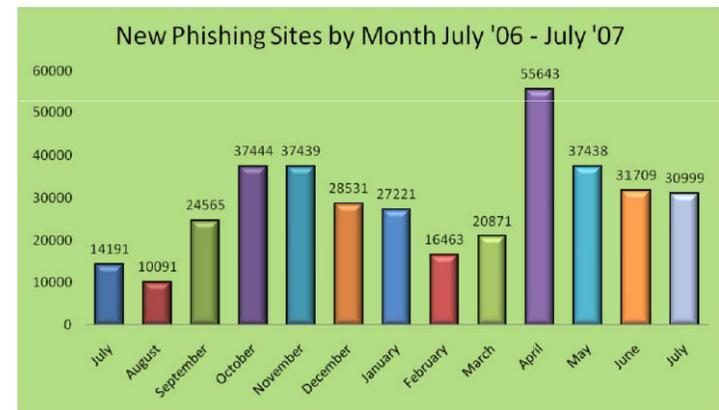
Pharming

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

¿Quién se ha comido mis datos?

Una parada para pensar...

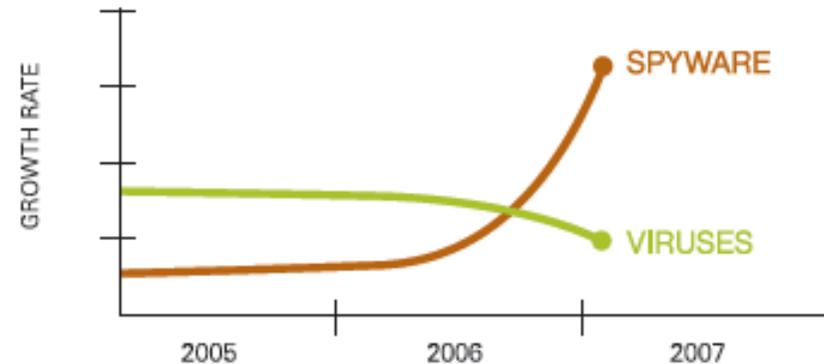
Luis Herreros Sánchez

Desarrollo de Negocio SATEC



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)



¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



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

From: <[REDACTED]>

Man you have got to tell me where you picked her up. I saw this on the web, it has to be you check it out yourself <http://www.youtube.com/watch?v=IHZbpJLfppV>

¿Quién se ha comido mis datos?

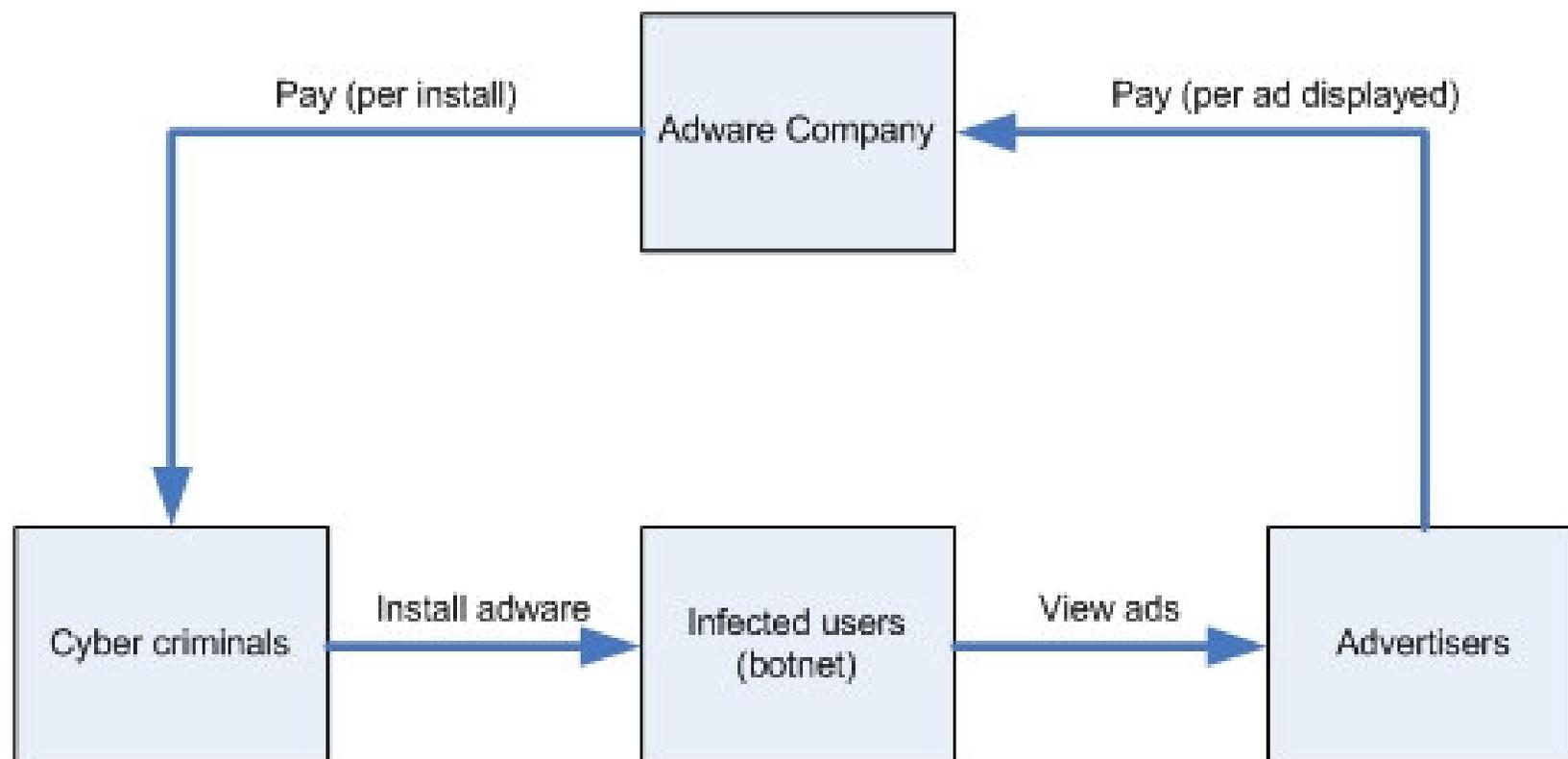
Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



Un caso de éxito...

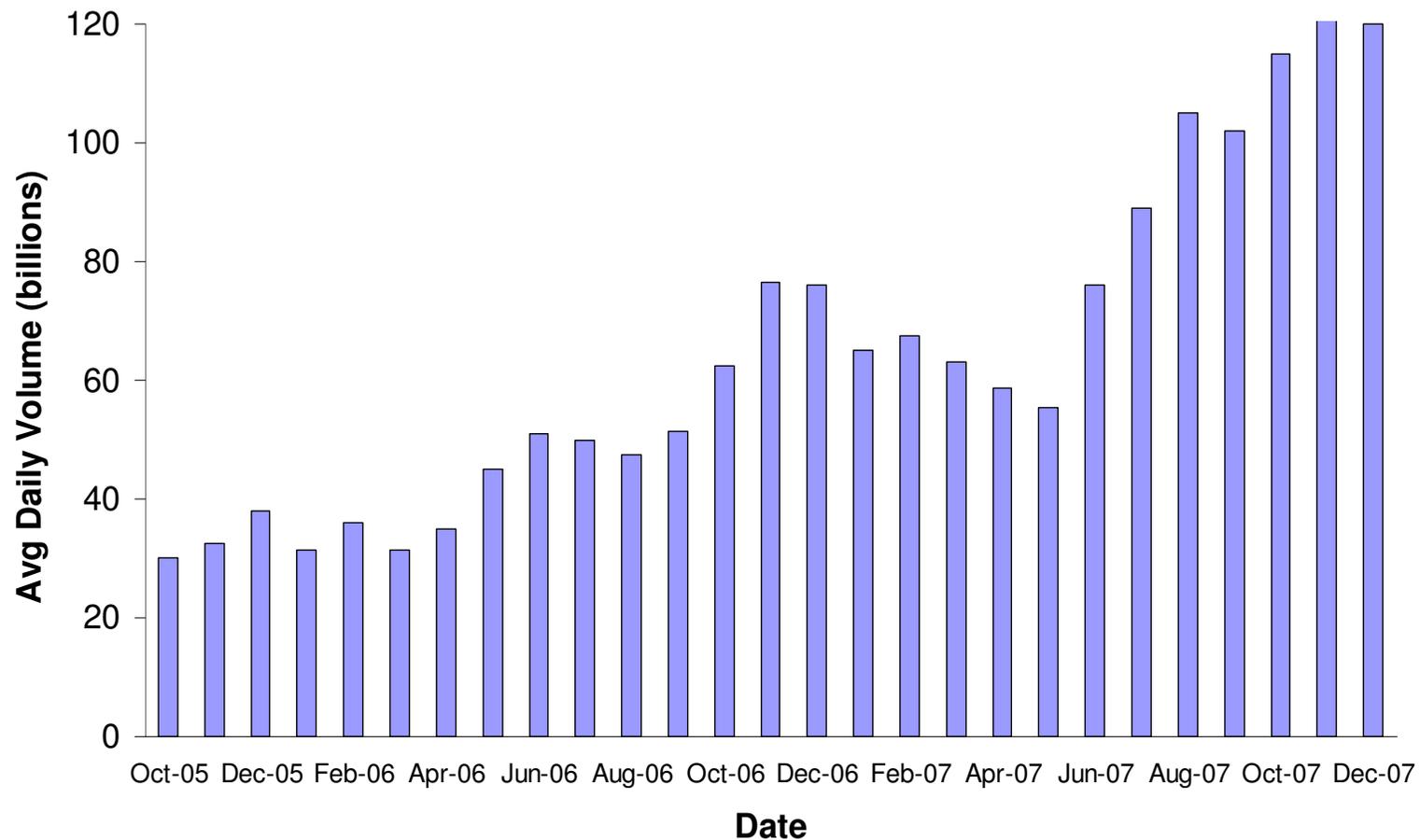


Los números...

- 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: $0.4 \times 5000 \times 8 = \$16,000$* (mensual)
- *Ganancias netas: \$15,843* (Primer mes)

¡El spam continúa creciendo!

¡x4 en 2 años!



¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



Spam de imágenes

Gran « innovación » de 2006 y principios de 2007

1. “Puntos Polca”

*****ATTENTION ALL DAY TRADERS AND INVESTORS*****

INVESTOR ALERT!
IT LOOKS LIKE ANOTHER RUN FOR SWNM!
WATCH SWNM LIKE A HAWK ON Tuesday July 1, 2006

Company Name: SOUTHWESTERN MEDICAL, INC.
Stock Symbol: SWNM
Monday Close: 0.11
Volume: 5,761,702
Change: UP 0.025 (27.78%)
Market Cap: \$33,000,000.00 (Approx)

Goldmark Industries, Inc (GDKI.PK)

THIS STOCK IS EXTREMELY UNDERVALUED
Huge Advertising Campaign this week!
Breakout Forecast for July, 2006

Current Price: \$5.60
Short Term Price Target: \$12.00
Recommendation: Strong Buy
***300+% profit potential short term**

RECENT HOT NEWS released MUST READ ACT NOW
LOS ANGELES_VANCOUVER, British Columbia -- Goldmark Industries, Inc. (GDKI.PK), the Company has recently signed a multi-movie distribution agreement with Mr. Rodriguez's production and distribution company, Polychrome Pictures, for the automatic theatrical and home video distribution of feature length films scheduled for release by Goldmark. Goldmark is making the most of the current market...

2. Cortes de imágenes

***** BREAKING NEWS ALERT ISSUED *****
***** BREAKING NEWS ALERT ISSUED *****

Most stock brokers give out their new issues only to their largest commission paying clients. We assume many of you like to "trade the promotion" and may have made some big, fast money doing so.

Trade Date : Monday, July 31, 2006
Company : EVER GLORY INTL INC
Ticker: EGLY
Rises Over 5% on Friday.
Volume: 270,947
Price at Close Friday: \$1.15
3-6 Day Trading: \$3 - \$4
Expectations : STRONG BUY

Looking for a company with some good news? Here's one!

Breaking News:
Ever-Glow Signs \$500,000 Deal with Debenhams (Read Yahoo Finance) There is a massive promotion underway this weekend apprising potential eager investors of this emerging situation.
Breaking news alert issue - big news coming. We feel this is a "Stock Alert" and you should have this on your Radar.
Big news expected. This should invoke LARGE gains. Do this often enough, and your portfolio can double, even TRIPLE in value.

*****BREAKING NEWS ALERT ISSUED*****
Most stock brokers give out their new issues only to their largest commission paying clients. We assume many of you like to "trade the promotion" and may have made some big, fast money doing so.

Trade Date : Friday, July 28, 2006
Company : EVER GLORY INTL INC
Ticker : EGLY
Price : \$1.09
3-6 Day Trading : \$3 - \$6
Expectations : BUY

Looking for a company with some good news? Here's one!

Breaking News:
Ever-Glory Signs \$500,000 Deal with Debenhams (Read Yahoo Finance)

There is a massive promotion underway this weekend apprising potential eager investors of this emerging situation.
Breaking news alert issue - big news coming. We feel this is a "Stock Alert" and you should have this on your Radar.

¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



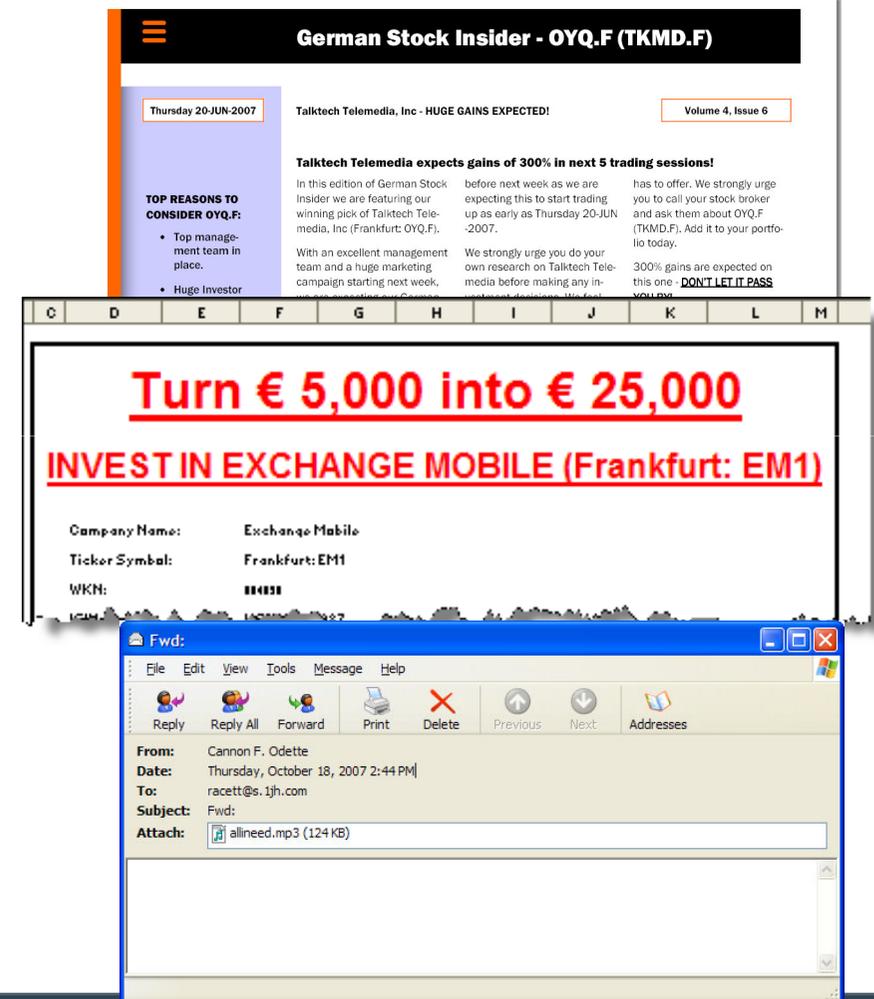
Otras técnicas de 2007

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.



¿Quién se ha comido mis datos?

Luis Herreros Sánchez

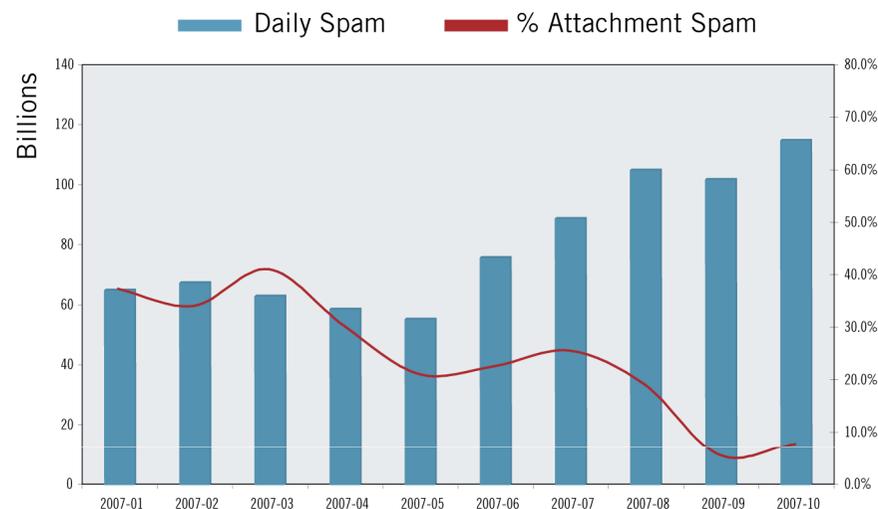
Una parada para pensar...

Desarrollo de Negocio SATEC

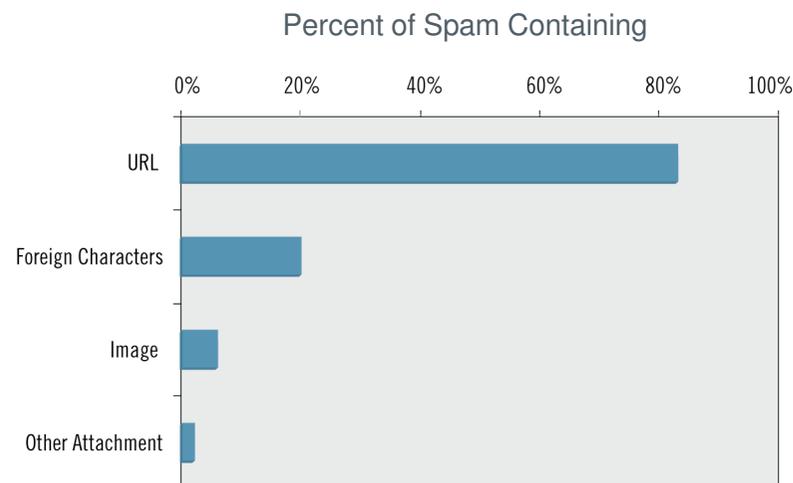


La nueva técnica: URL spam

De las imágenes a los enlaces web



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



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

¿Quién se ha comido mis datos?

Una parada para pensar...

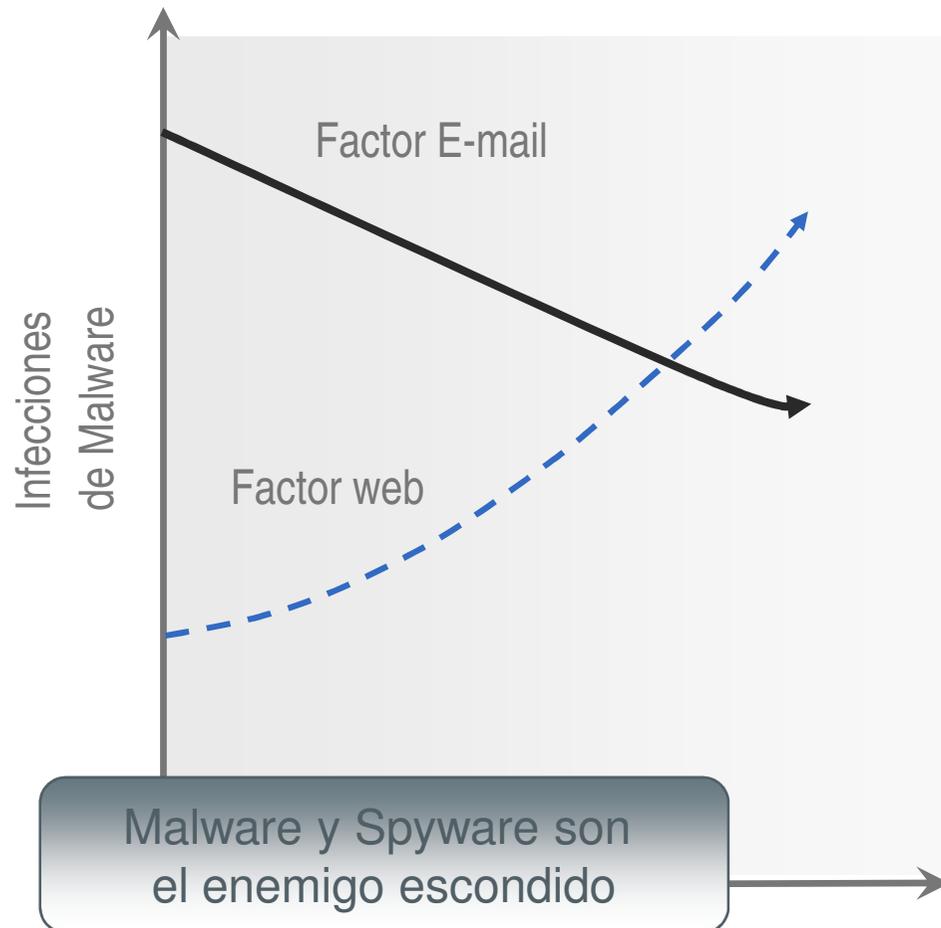
Luis Herreros Sánchez

Desarrollo de Negocio SATEC



Factores de amenazas de malware

Cambiando del e-mail a la web



TD Ameritrade Breach Affects 6.3M Customers

Brokerage firm uncovers data-sucking malware during system audit

From: <[redacted]@tdameritrade.com>

Man you have got to tell me where you picked her up. I saw this on the web, it has to be you. check it out yourself <http://www.youtube.com/watch?v=IHZbpJLfppV>

YouTube
Broadcast Yourself™
Your Download Should Begin Shortly. If your download does not start in approximately 15 seconds you can [click here](#) to launch the download and then press Run.
This site is not affiliated with YouTube.
<http://www.networkworld.com/news/2007/020207-dolphins-web-sites-hacked-in.html>

Dolphins' Web sites hacked in advance of Super Bowl

By Rob [redacted]



IT Week > News > Hacking

Smart malware steals from SSL streams

Is nothing safe?

Iain Thomson, vnunet.com, 22 May 2007



A new variant of this malware is stealing data

¿Quién se ha comido mis datos?

Luis Herreros Sánchez

Una parada para pensar...

Desarrollo de Negocio SATEC



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

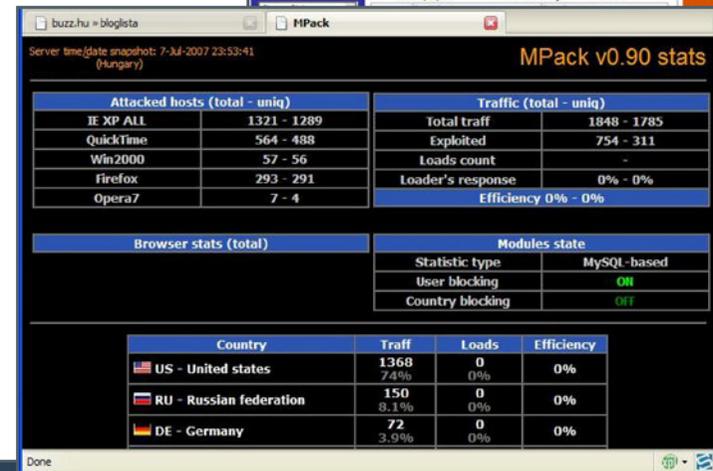
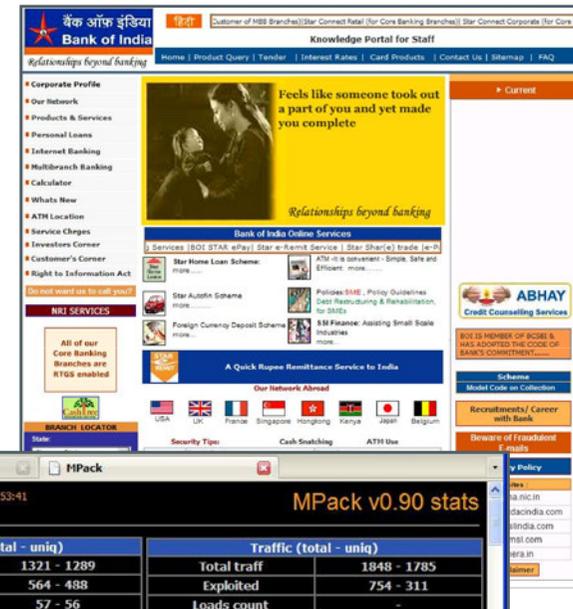
- Sitios web legítimos se convierten en puntos de distribución

–Ataques iFrame

–Miami Dolphins, Bank of India

–Hack masivo Mpack

- Los usuarios introducen el malware dentro de la red



¿Quién se ha comido mis datos?

Luis Herreros Sánchez

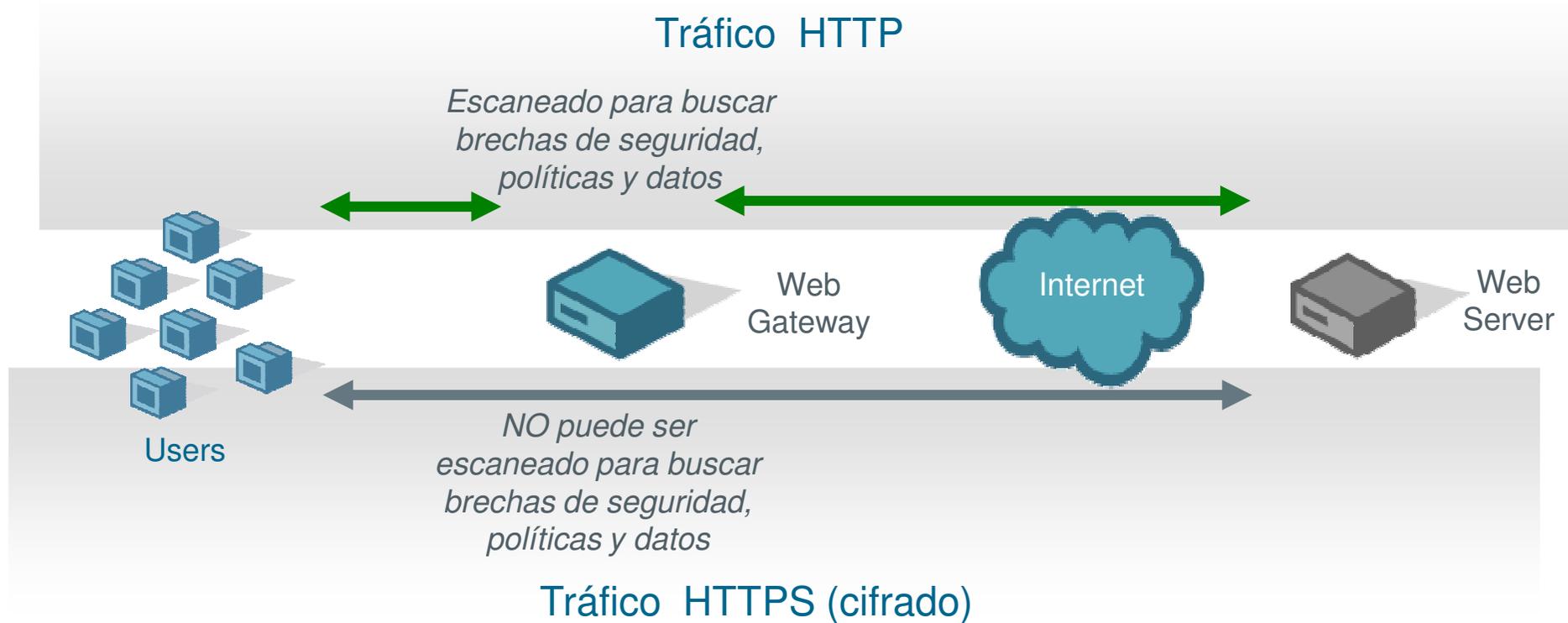
Una parada para pensar...

Desarrollo de Negocio SATEC



HTTPS

Un punto ciego para las empresas



¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



LO QUE HEMOS APRENDIDO

¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC

43



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?

¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



¿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.



¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



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

¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



¿APAGAMOS LOS ORDENADORES?

¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC

47



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



¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



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

¿Quién se ha comido mis datos?

Una parada para pensar...

Luis Herreros Sánchez

Desarrollo de Negocio SATEC



Podemos unir ambos enfoques



¿Quién se ha comido mis datos?

Una parada para pensar...

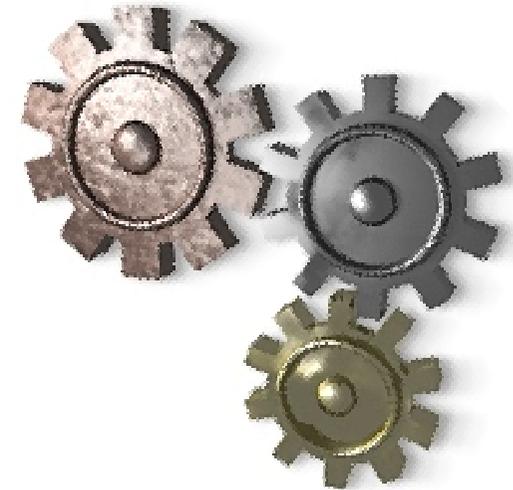
Luis Herreros Sánchez

Desarrollo de Negocio SATEC



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

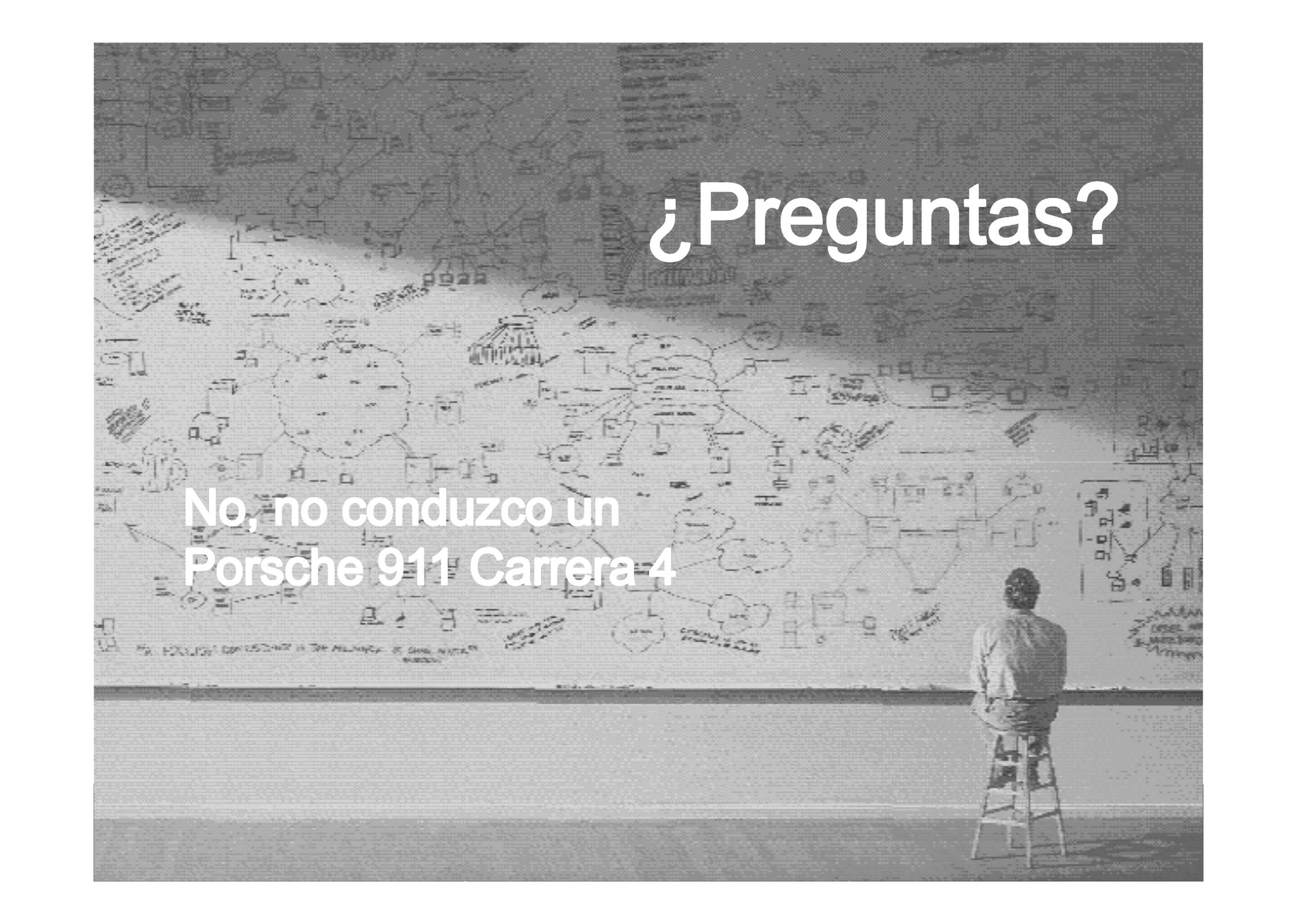
- Sistema de Gestión de Seguridad de la Información
 - Es un plan de mejora continua.
 - Tiene un alcance definido a la medida de la organización.
 - Utiliza análisis de riesgos y métricas de seguimiento.
 - Está vivo.
 - Se puede basar en estándares.
 - Se puede certificar.
- Cualquier sistema de gestión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



A black and white photograph of a person sitting on a stool, looking at a large wall covered in complex diagrams and sketches. The diagrams include flowcharts, mind maps, and various technical drawings. The person is seen from behind, wearing a light-colored jacket and dark pants. The wall is filled with intricate lines and shapes, suggesting a detailed engineering or design process.

¿Preguntas?

No, no conduzco un
Porsche 911 Carrera 4



Muchas Gracias

Luis Herreros Sánchez

lhsanchez@satec.es