CENTRO CRIPTOLÓGICO NACIONAL

INSTITUTO JUAN VELÁZQUEZ DE VELASCO
de Investigación en Inteligencia para la Seguridad y la Defensa
Universidad Carlos III de Madrid

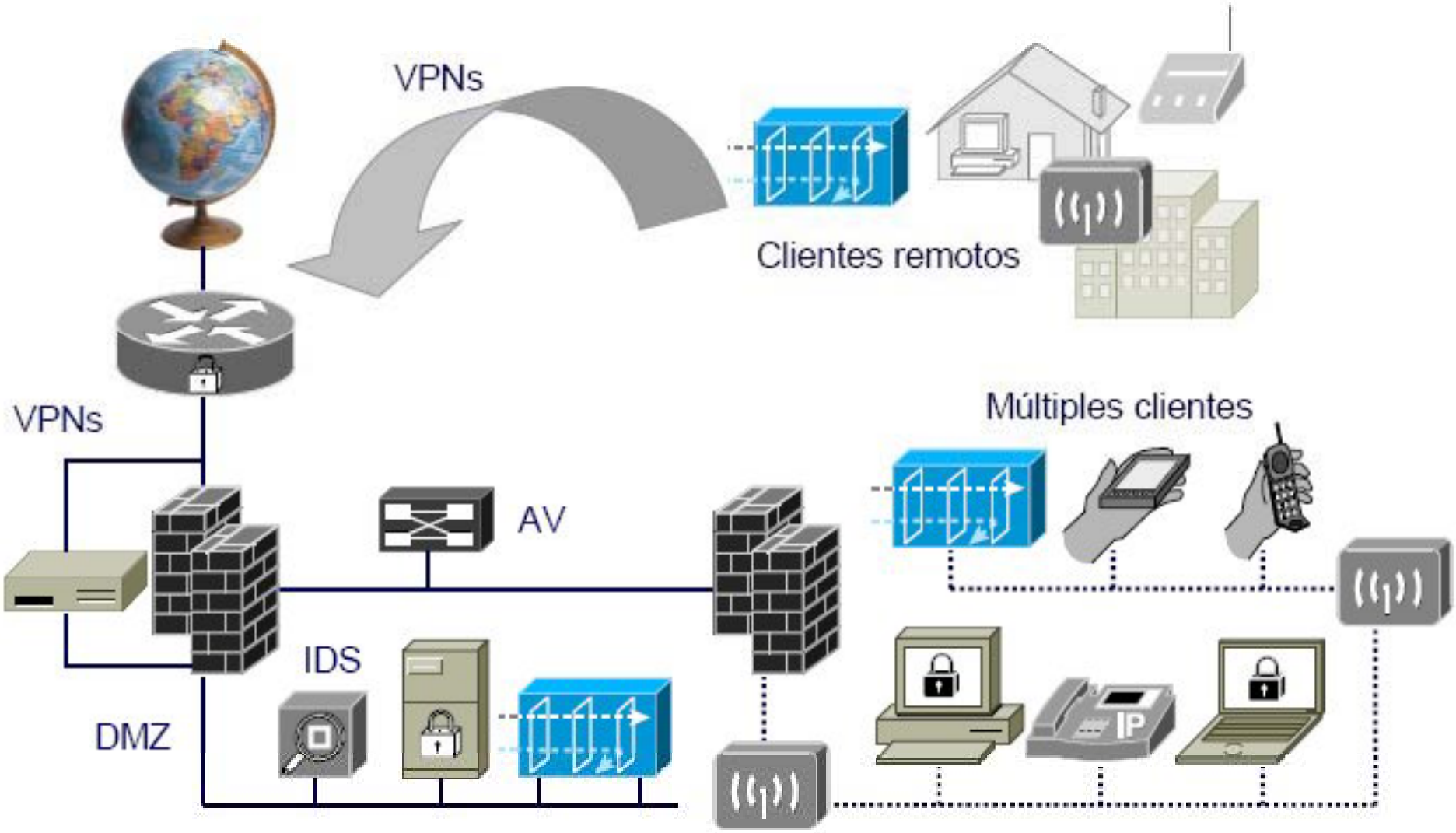
Nuevas Amenazas y Nuevas Tecnologías:

Los Servicios de Inteligencia frente a la Red

Campus de Colmenarejo, 22 marzo de 2007

Nuevas Amenazas y Nuevas Tecnologías: Los Servicios de Inteligencia frente a la Red

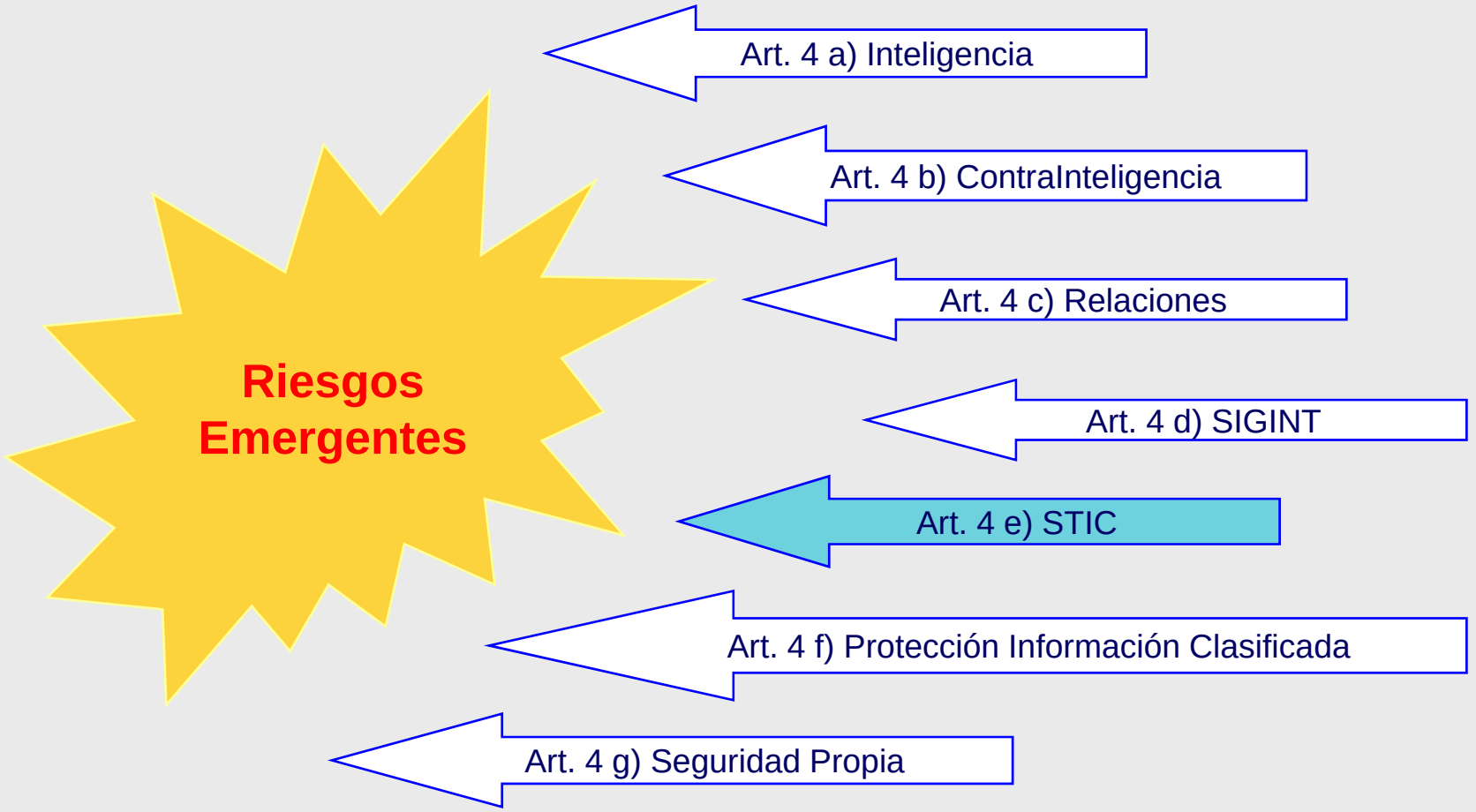
- **CENTRO CRIPTOLÓGICO NACIONAL**
  - **QUÉ ES EL CCN?**
- **ACTIVIDAD DEL CCN**
  - **A QUÉ SE DEDICA EL CCN?**
- **NUEVAS AMENAZAS Y NUEVAS TECNOLOGÍAS**
  - **QUIÉN ES EL AGRESOR?**
  - **CUALES SON LAS TECNICAS DE AGRESIÓN?**


VPNs
Clientes remotos
VPNs
Múltiples clientes
AV
IDS
DMZ
IP

Exposición de Motivos (Ley 11/2002)

- La sociedad española demanda unos Servicios de Inteligencia eficaces, especializados y modernos, capaces de afrontar los nuevos retos del actual escenario nacional e internacional, regidos por los principios de control y pleno sometimiento al ordenamiento jurídico.
- … los nuevos retos que para los servicios de inteligencia se derivan de los llamados riesgos emergentes, que esta Ley afronta al definir las funciones del Centro …

Centro Nacional de Inteligencia (Ley 11/2002)



Funciones del CNI (Ley 11/2002)

- (Capítulo I, Artículo 4º, apartado e) **Coordinar** la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, **garantizar** la seguridad de las tecnologías de la información en ese ámbito, **informar** sobre la adquisición coordinada de material criptológico y **formar** a personal, propio o de otros servicios de la Administración, especialista en este campo para **asegurar el adecuado cumplimiento de las misiones del Centro.**

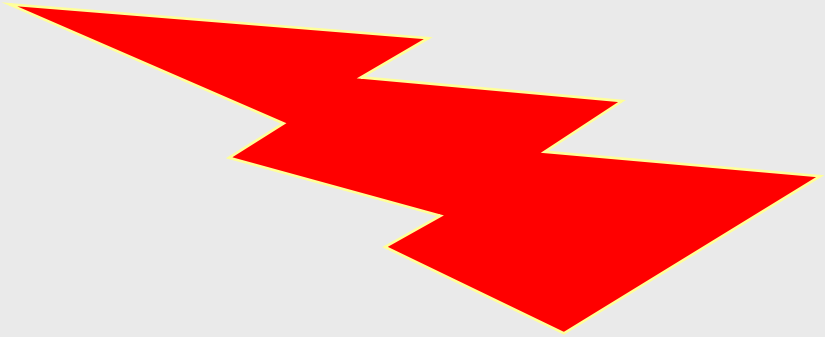
- (Capítulo I, Artículo 4º, apartado f) **Velar** por el cumplimiento de la normativa relativa a la protección de la información clasificada.

Funciones del CCN (RD 421/2004)

- **Elaborar y difundir** normas, instrucciones, guías y recomendaciones para garantizar la seguridad de las TIC en la Administración.
- **Formar** al personal de la Administración especialista en el campo de la seguridad de las TIC.
- Constituir el **organismo de certificación** del Esquema Nacional de Evaluación y Certificación de aplicación a productos y sistemas de su ámbito.
- **Valorar y acreditar** capacidad productos de cifra y Sistemas de las TIC (incluyan medios de cifra) para manejar información de forma segura.
- Coordinar la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación y la utilización de la **tecnología de seguridad** de los Sistemas antes mencionados.
- Velar por el cumplimiento normativa relativa a la protección de la **información clasificada** en su ámbito de competencia (Sistemas de las TIC)
- Establecer las necesarias **relaciones** y firmar los acuerdos pertinentes con organizaciones similares de otros países,
- Para el desarrollo de las funciones mencionadas. Coordinación oportuna con las Comisiones Nacionales a las que la leyes atribuyan responsabilidades en el ámbito de los sistema de las Tecnologías de la Información y de las Comunicaciones.

Seguridad de las Tecnologías de la Información (STIC)

- La seguridad de las Tecnologías de la Información es la capacidad de las propias TI para evitar, hasta un determinado nivel de confianza, el compromiso de la confidencialidad, integridad y disponibilidad de la información que procesan, almacenan o transmiten (manejan) los sistemas y la integridad y disponibilidad de los propios sistemas



¿Cómo se logra la STIC?

- **Mediante un Conjunto de Medidas**
- la complejidad de los actuales sistemas CIS impide garantizar su seguridad con absoluta certeza.

- La aplicación e implementación de medidas de protección en las TI pretende conseguir un nivel de seguridad aceptable, *valorando y asumiendo un nivel de riesgos conocidos.*

- Un nivel de seguridad aceptable se logra con la combinación equilibrada de medidas de distinta naturaleza y su constante revisión. Entre dichas medidas destacan:
  - Información y Formación
  - Medidas políticas y organizativas
  - Requisitos y Procedimientos
  - Medidas técnicas de protección

¿En qué trabaja el CCN?

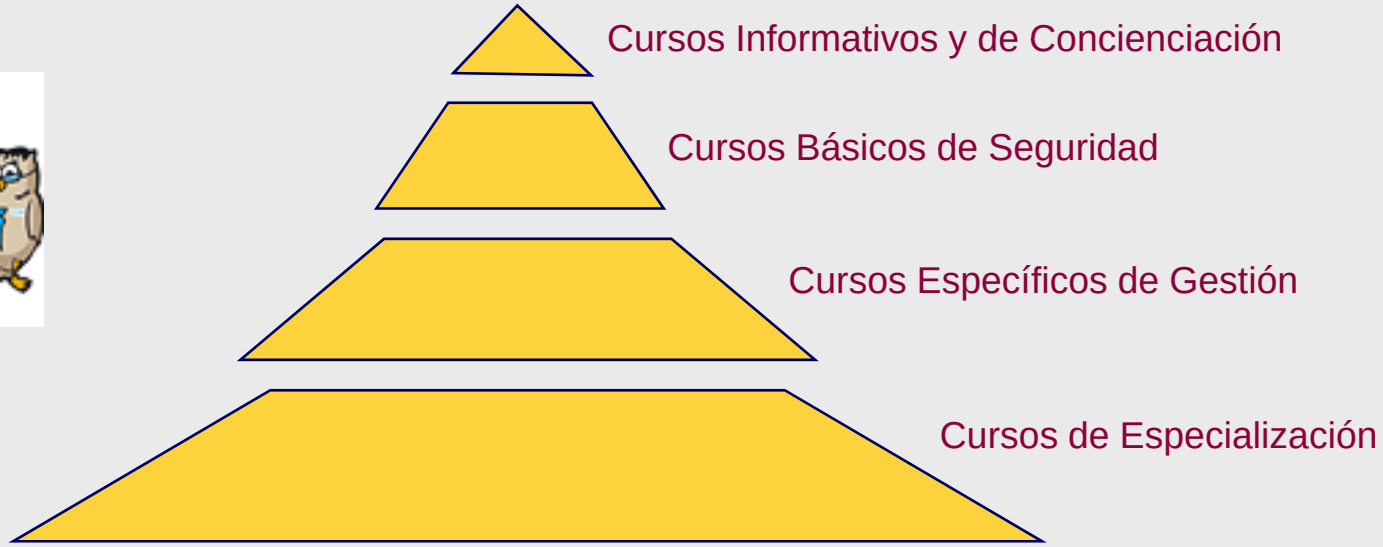
- Información y Formación
- Medidas políticas y organizativas
- Requisitos y Procedimientos
- Medidas técnicas de protección
- Gestión y Respuesta ante Incidentes de Seguridad de las TIC

Y qué hace?

- Elaborar y difundir normas, instrucciones y guías
- Formar en seguridad TI
- Certificar la seguridad de productos TI
- Valorar y acreditar la seguridad de Sistemas
- Promocionar el desarrollo y el uso de la tecnología de seguridad
- Velar por el cumplimiento de las normas de seguridad TI
  - Auditorías e inspecciones

Funciones CCN (Formación)

Formar al personal de la Administración especialista en el campo de la seguridad de los sistemas de las tecnologías de la información y las comunicaciones.



Funciones CCN (Formación)

- Algunos Datos (2005-2006)
  - 56 organismos diferentes de la Administración (General Autonómica y Local)
  - 307 funcionarios
  - 1300 horas lectivas

Funciones CCN (Normativa)

Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los Sistemas de las tecnologías de la información y las comunicaciones de la Administración

- CCN-STIC 000: Instrucciones/Políticas STIC
- CCN-STIC 100: Procedimientos
- CCN-STIC 200: Normas
- CCN-STIC 300: Instrucciones Técnicas
- CCN-STIC 400: Guías Generales
- CCN-STIC 500: Guías Entornos Windows
- CCN-STIC 600: Guías Otros Entornos
- CCN-STIC 900: Informes Técnicos

Series CCN-STIC: Un Ejemplo

- **Serie 400: Guías Generales**
  - CCN-STIC-401 Glosario / Abreviaturas
  - CCN-STIC-402 Organización y Gestión TIC
  - CCN-STIC-403 Gestión de Incidentes de Seguridad
  - CCN-STIC-404 Control de Soportes Informáticos
  - CCN-STIC-405 Algoritmos y Parámetros de Firma Electrónica
  - CCN-STIC-406 Seguridad Wireless
  - CCN-STIC-407 Seguridad en Telefonía Móvil
  - CCN-STIC-408 Seguridad en Cortafuegos
  - CCN-STIC-409 Protección física de equipos
  - CCN-STIC-410 Análisis de Riesgos en Sistemas de la Administración
  - CCN-STIC-430 Herramientas de Seguridad
  - CCN-STIC-431 Herramientas de Análisis de Vulnerabilidades
  - CCN-STIC-432 Herramientas de Detección de Intrusos
  - CCN-STIC-433 Herramientas de Detección de SW Dañino
  - CCN-STIC-434 Herramientas de Análisis de Auditoría
  - CCN-STIC-435 Herramientas de Monitorización del Tráfico
  - CCN-STIC-436 Herramientas que Mejoran la Seguridad
  - CCN-STIC-437 Herramientas de Cifrado SW
  - CCN-STIC-438 Herramientas de Esteganografía
  - CCN-STIC-450 Seguridad TEMPEST

Series CCN-STIC

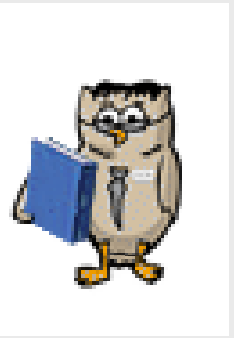
- **Serie 500: Guías para Entornos Windows**
  - CCN-STIC-501 Seguridad en Windows XP SP2
  - CCN-STIC-502 Seguridad en Clientes Windows
  - CCN-STIC-503 Seguridad en Windows 2003 Server
  - CCN-STIC-504 Seguridad en Internet Information Server
  - CCN-STIC-505 Seguridad en BD SQL
  - CCN-STIC-506 Seguridad en MS Exchange
  - CCN-STIC-507 Seguridad ISA Server
  - CCN-STIC-508 Seguridad en Clientes W2000
  - CCN-STIC-509 Seguridad en Windows XP Embedded
  - CCN-STIC-510 Seguridad en Windows CE
  - CCN-STIC-511 Seguridad W2003 Server (Servidor de Ficheros)
  - CCN-STIC-512 Seguridad en Windows 2003 (Servidor Impresión)
  - CCN-STIC-513 Seguridad DNS
  - CCN-STIC-514 Gestión de Parches de Seguridad en Sistemas Windows
  - CCN-STIC-515 Control de Integridad en sistemas WINDOWS
  - CCN-STIC-516 Auditoría de seguridad en sistemas WINDOWS

- **Serie 600: Guías para Otros Entornos**
  - CCN-STIC-601 Configuración de Seguridad HP-UX v 10.20
  - CCN-STIC-602 Configuración de Seguridad HP-UX 11i
  - CCN-STIC-610 Configuración de Seguridad Red Hat Linux
  - CCN-STIC-611 Configuración de Seguridad SUSE linux
  - CCN-STIC-612 Configuración de Seguridad DEBIAN
  - CCN-STIC-621 Configuración de Seguridad Sun-Solaris 8.0
  - CCN-STIC-622 Configuración de Seguridad Sun-Solaris 9.0 para ORACLE
  - CCN-STIC-623 Configuración de Seguridad Sun-Solaris 10.0 para ORACLE
  - CCN-STIC-624 Configuración de Seguridad Sun-Solaris 9.0 con NFS
  - CCN-STIC-625 Configuración de Seguridad Sun-Solaris 10.0 con NFS
  - CCN-STIC-626 Configuración de Seguridad Sun-Solaris 9.0 Estación de trabajo
  - CCN-STIC-627 Configuración de Seguridad Sun-Solaris 10.0 Estación de trabajo
  - CCN-STIC-631 Seguridad en BD Oracle
  - CCN-STIC-641 Seguridad en Equipos de Comunicaciones
  - CCN-STIC-651 Seguridad en entornos LOTUS
  - CCN-STIC-671 Seguridad de Servidor WEB APACHE

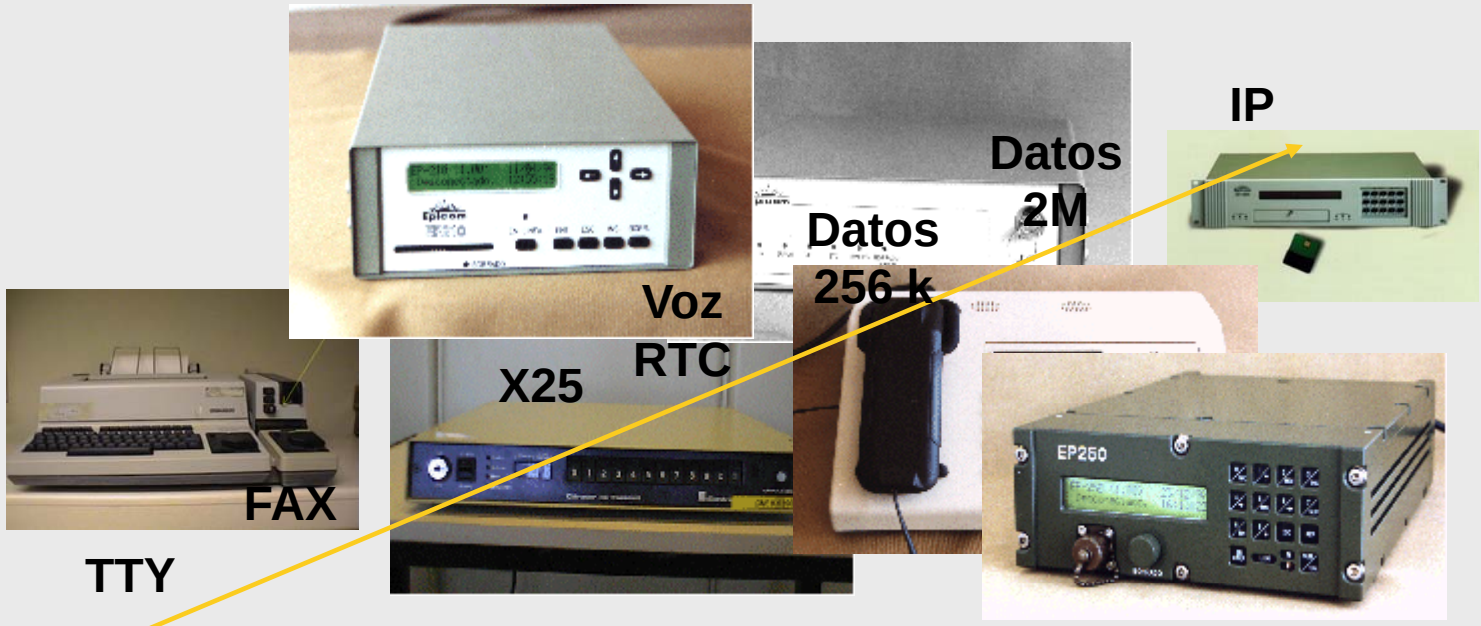
Funciones CCN (Certificación)

Constituir el organismo de certificación del Esquema Nacional de Evaluación y Certificación de aplicación a productos y sistemas de su ámbito

- CERTIFICACIÓN
  - CRIPTOLOGICA
    - Lista de productos certificados (Secreto/ Reservado/ Confidencial/ Difusión Limitada)
  - FUNCIONAL DE SEGURIDAD Common Criteria e ITSEC
    - EAL1 a EAL7 y E1 a E7
  - RIESGO TEMPEST
    - Zonificación (Clases 0 -3)
    - Equipos y Plataformas (Clase 3 - 0)



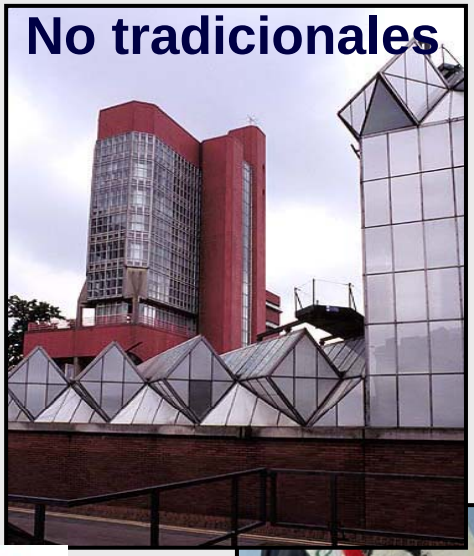
Certificación Criptológica – Productos de Cifra

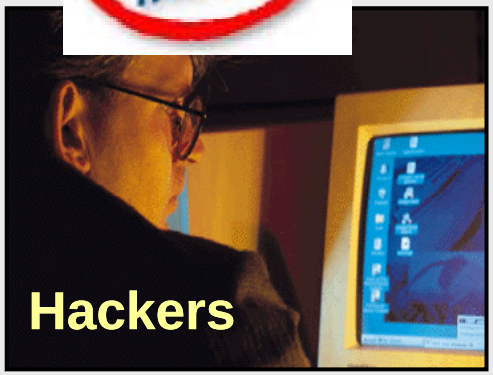


Más de 50 cifradores certificados (voz, fax, datos, IP, PKI)

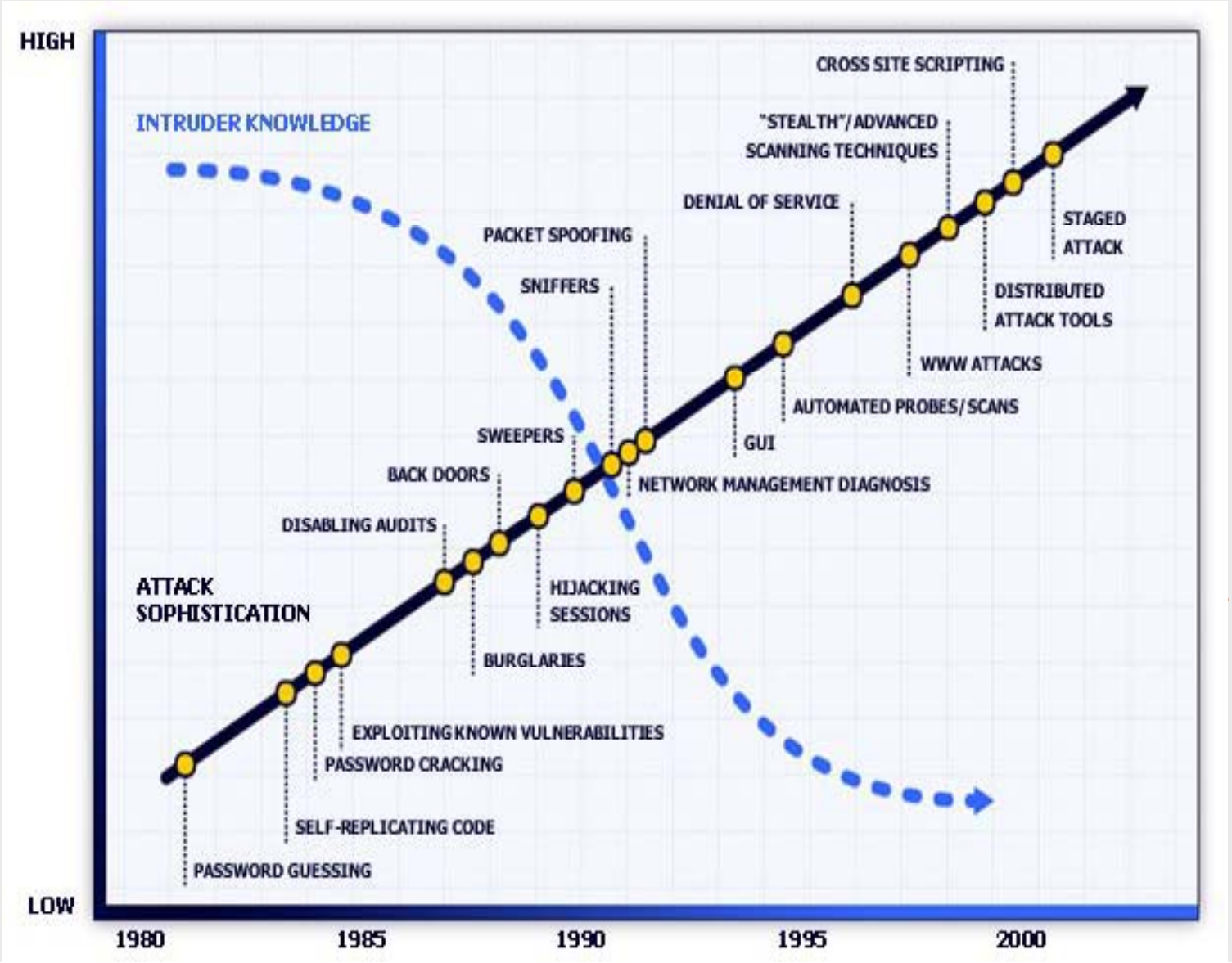
¿A QUIÉN Y A QUÉ NOS ENFRENTAMOS? EL AGRESOR

Fuentes de Amenaza Actual





EL AGRESOR – Principales Agresiones – Conocimientos agresor



CENTRO CRIPTOLÓGICO NACIONAL

CONVERGENCIA ENTRE AGENTES DE LA AMENAZA

El Agresor

U.S. Department of Justice
Federal Bureau of Investigation

For Immediate Release
August 26, 2005

Washington D.C.
FBI National Press Office

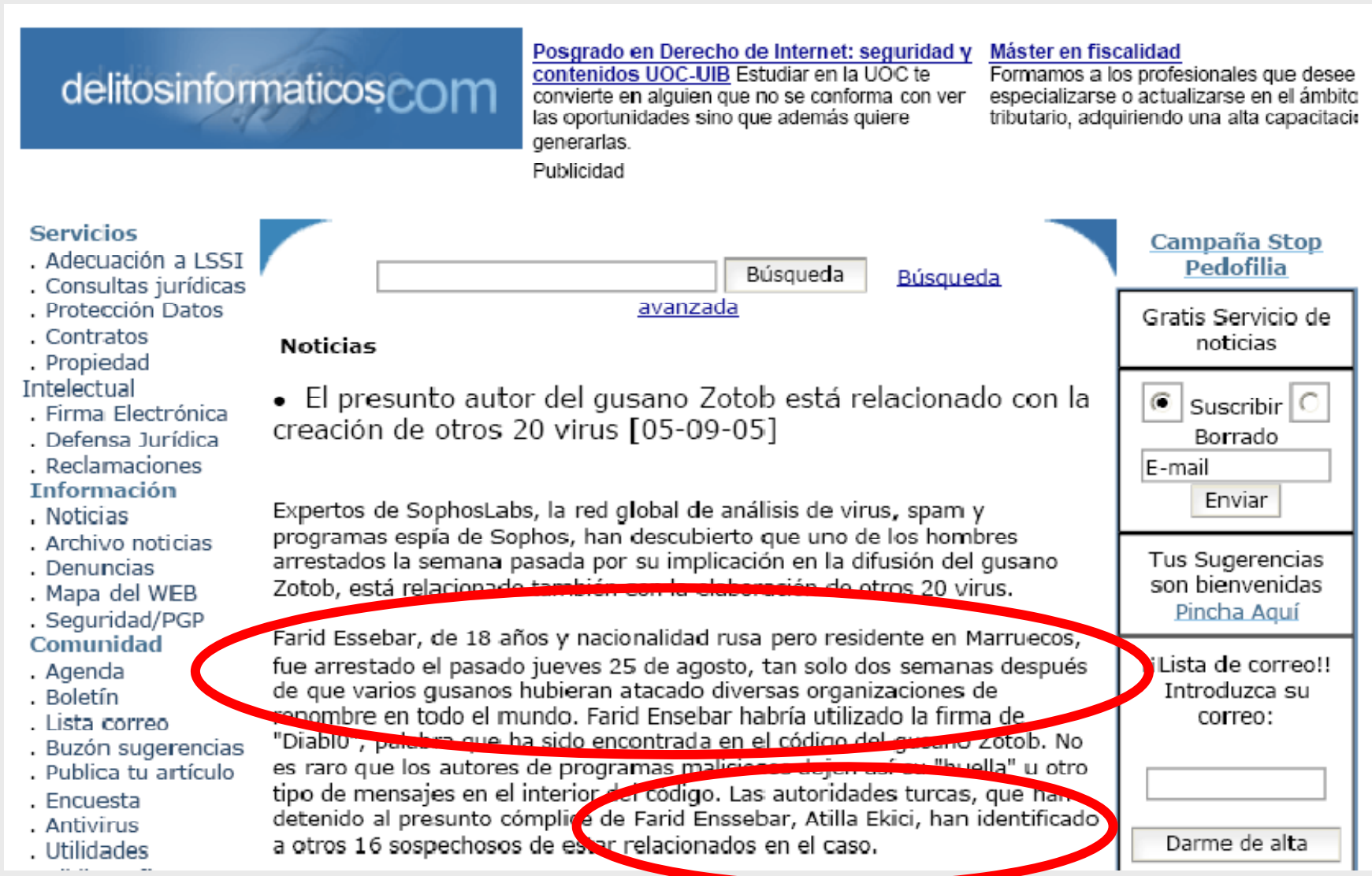
FBI ANNOUNCES TWO ARRESTS IN MYTOB AND ZOTOB COMPUTER WORM INVESTIGATION

Washington, D.C. - Working with law enforcement authorities in Morocco and Turkey, the FBI today announced the arrests of two individuals believed to be responsible for the creation and distribution of the "Mytob" and "Zotob" computer worms that were unleashed less than two weeks ago and disrupted services on computer networks of a variety of companies including major U.S. news organizations.

With the help of Moroccan authorities, Ministry of Interior Turkish National Police , and valuable assistance from Microsoft Corporation, these individuals were arrested yesterday without incident. Arrested in Morocco was Farid Essebar, 18, a Moroccan national born in Russia who went by the screen moniker "Diabl0." Arrested in Turkey was Atilla Ekici, aka "Coder," a 21-year old resident of Turkey. Both individuals will be subject to local prosecutions.

FBI Cyber Division Assistant Director Louis M. Reigel III said, "In today's world of

Farid Enssebar y Atilla Ekici



Yihad electrónica

Google

La Web Imágenes Grupos Directorio Noticias más »

e-jihad Búsqueda Búsqueda Avanzada Preferencias

Búsqueda: la Web páginas en español páginas de España

La Web Resultados **1** - **10** de aproximadamente **57.000** de **e-jihad**. (**0,30** segundos)

e-Jihad against Western Business - [Traduzca esta página]
e-jihad against Western business. ... **e-Jihad** against Western Business. by Giles Trendle. this article originally appeared on IT-Director.com on 5th April ...
www.globalprofile.co.uk/31 - 21k - En caché - Páginas similares

ANSA.it - Anp: accordo con Hamas e Jihad
L'annuncio dell' intesa, fatta anche con Hamas **e Jihad**, e' stato oggi ai membri del Quartetto (Usa, Ue, Russia e Onu). Lo hanno riferito fonti stampa ...
www.ansa.it/main/notizie/awnplus/ topnews/news/2005-10-30_1833383.html - 55k - En caché - Páginas similares

Mideast hackers may strike US sites, FBI warns | CNET News.com - [Traduzca esta página]
The cyberwar, dubbed "**E-jihad**" by pro-Palestinians, was sparked last month by the violence in Israel. More than 150 people, most of them Palestinian, ...
news.cnet.com/news/0-1007-200-3359667.html - 49k - 8 Nov 2005 - En caché - Páginas similares

Don't Freak Out Over 'E-Jihad' - [Traduzca esta página]
Unless you're a specific target it's not worth focusing on unsubstantiated general warnings. The world is full of threats.
www.eweek.com/article2/0,1895,1639427,00.asp - 85k - En caché - Páginas similares

LAS TÉCNICAS DE AGRESIÓN

AGRESIONES A LA T

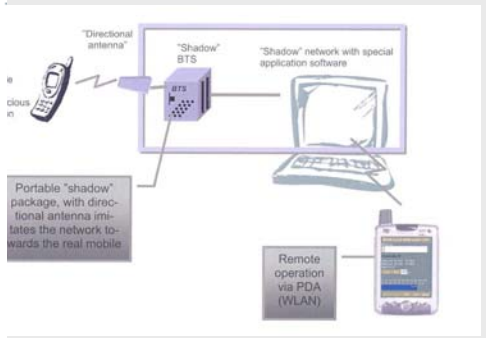
- Intercepta
  - Mala g
    Interc
  - Estadí
    - Al
      (1
      30
- Autentica
  activos
- Grabació
- Localizac
- Código da

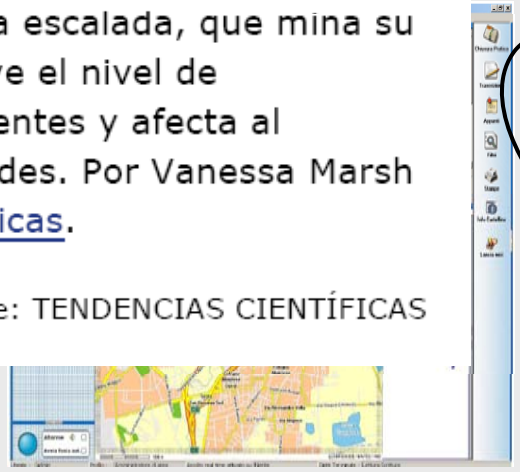
SEGURIDAD & MÓVILES

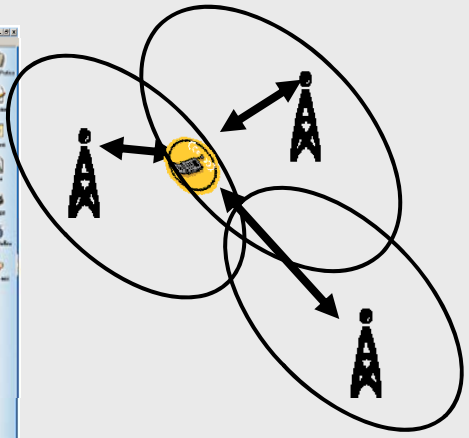
El 83% de las operadoras acusan ataques informáticos contra los móviles

El 83% de las operadoras denuncian ataques informáticos contra los teléfonos móviles, habiéndose detectado hasta 400 virus especializados en estos terminales. Los ataques de troyanos, virus y spyware contra móviles se quintuplicaron en 2006, según una investigación realizada por McAfee. El 80% de las operadoras expresan su preocupación por esta escalada, que mina su credibilidad, disminuye el nivel de satisfacción de los clientes y afecta al rendimiento de las redes. Por Vanessa Marsh de Tendencias Científicas.

21 Feb 2007, 09:35 | Fuente: TENDENCIAS CIENTÍFICAS

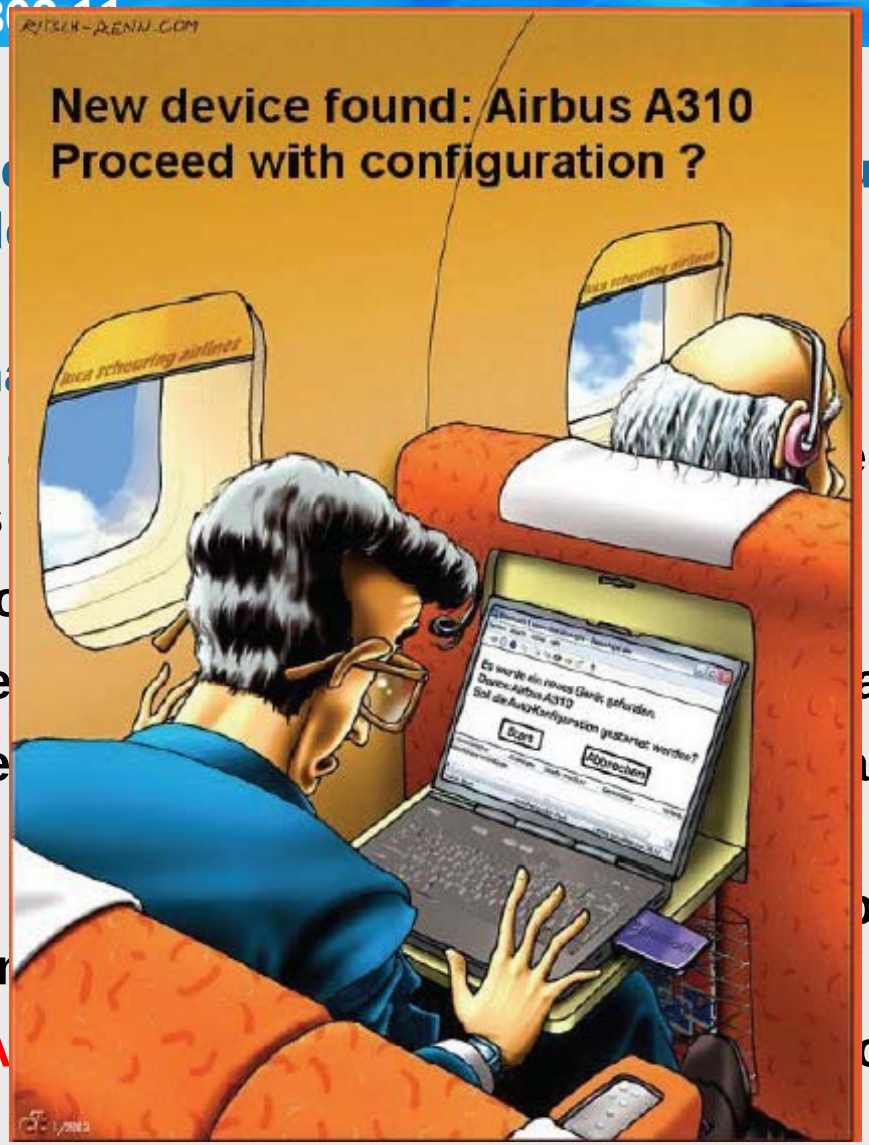




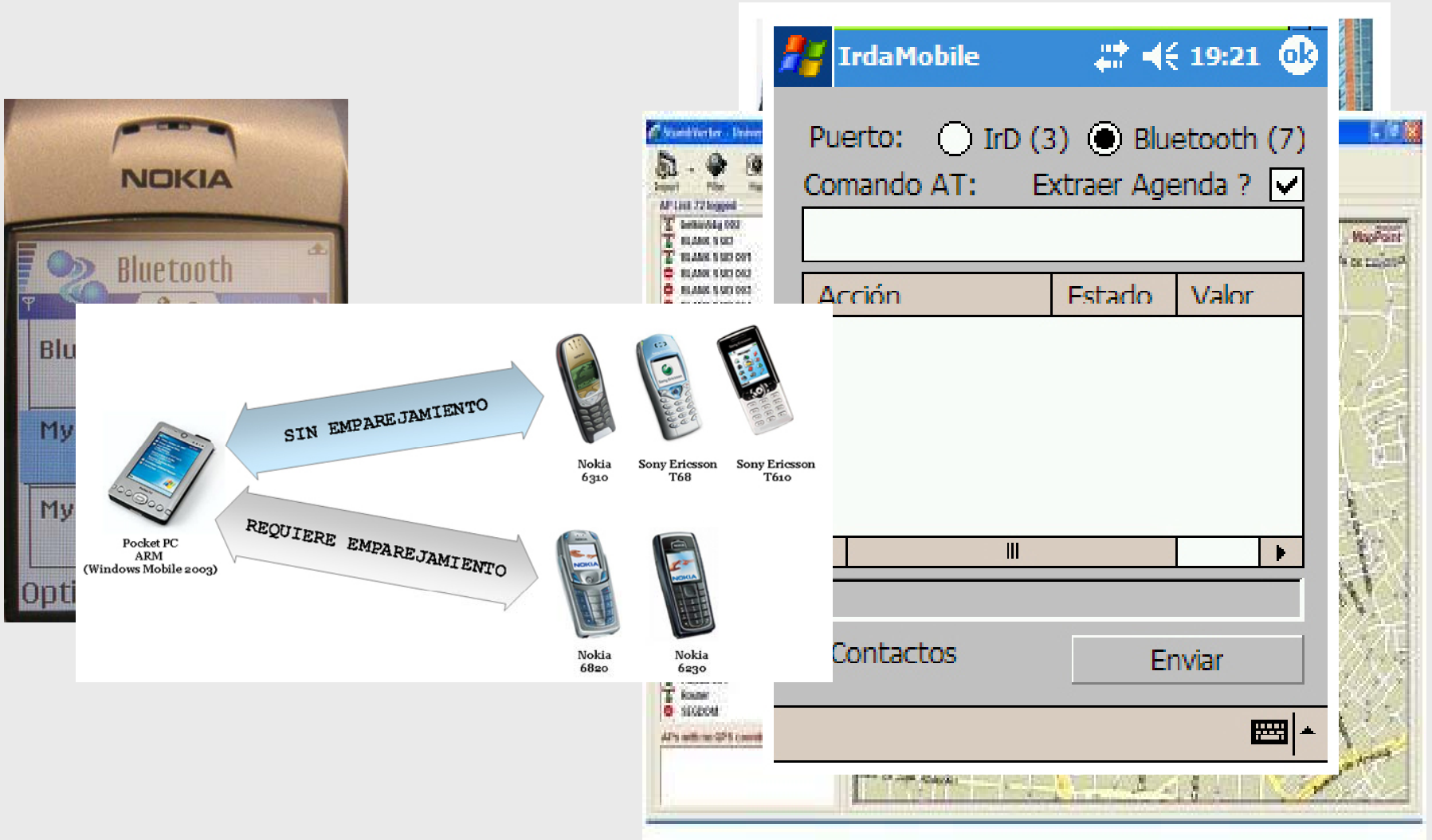


Agresiones en Redes 80

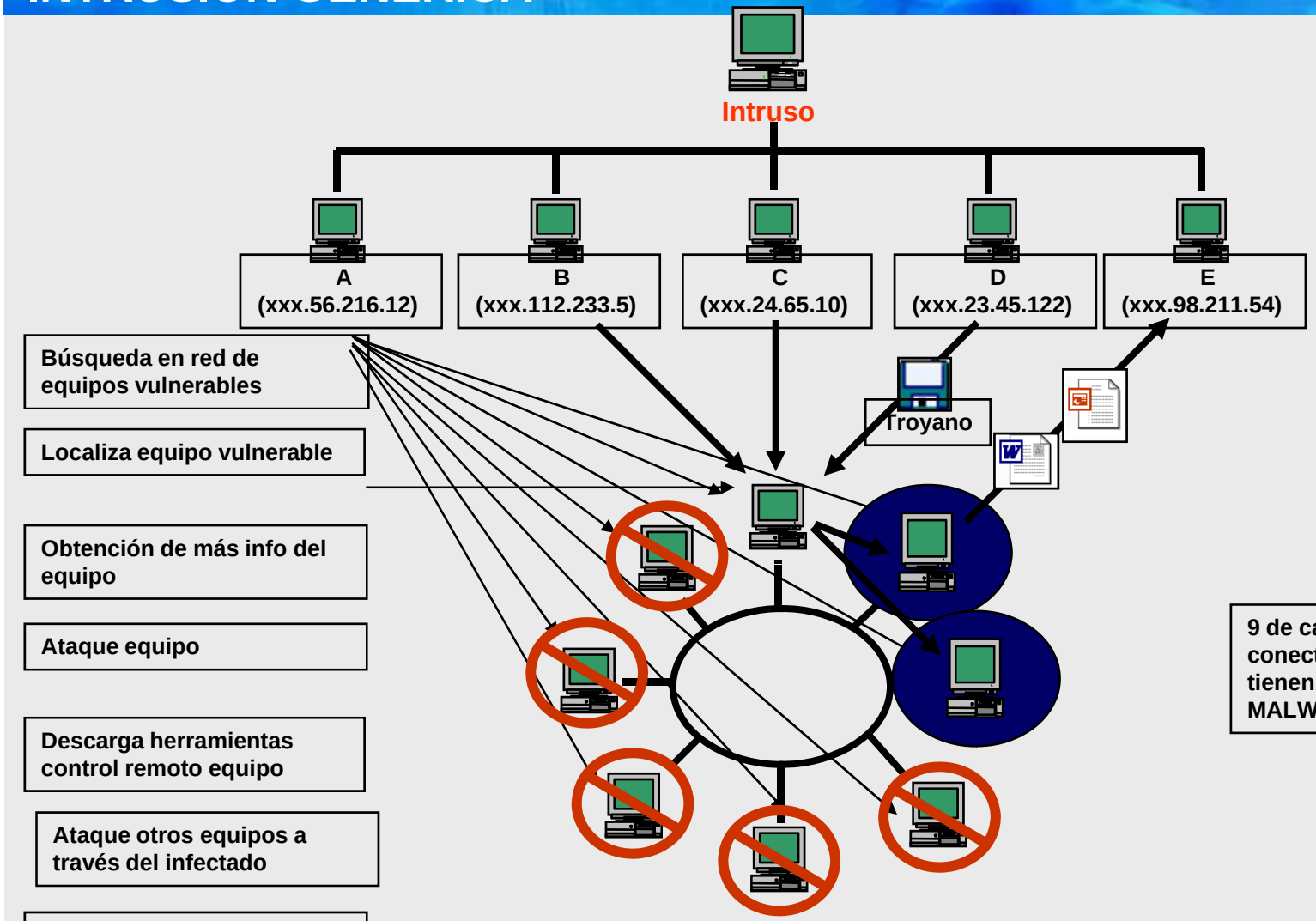
- Los Amenazas d uma de todas los que afectan a red introducidos por esta tecnología.
- Principales amen
  - Los datos ptibles de ser interceptados
  - Se pueden pr
  - Se puede inye a gran distancia.
  - Se pueden de aques de “Man in the Middle”.
  - Se pueden olegando Redes Inalámbricas r
  - La SEGURIDA opcional.



Redes inalámbricas (WIRELESS)



INTRUSIÓN GENÉRICA



Búsqueda en red de equipos vulnerables

Localiza equipo vulnerable

Obtención de más info del equipo

Ataque equipo

Descarga herramientas control remoto equipo

Ataque otros equipos a través del infectado

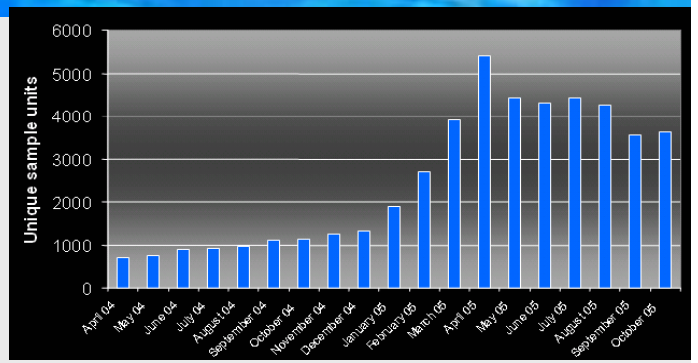
Extracción de información a través de este equipo

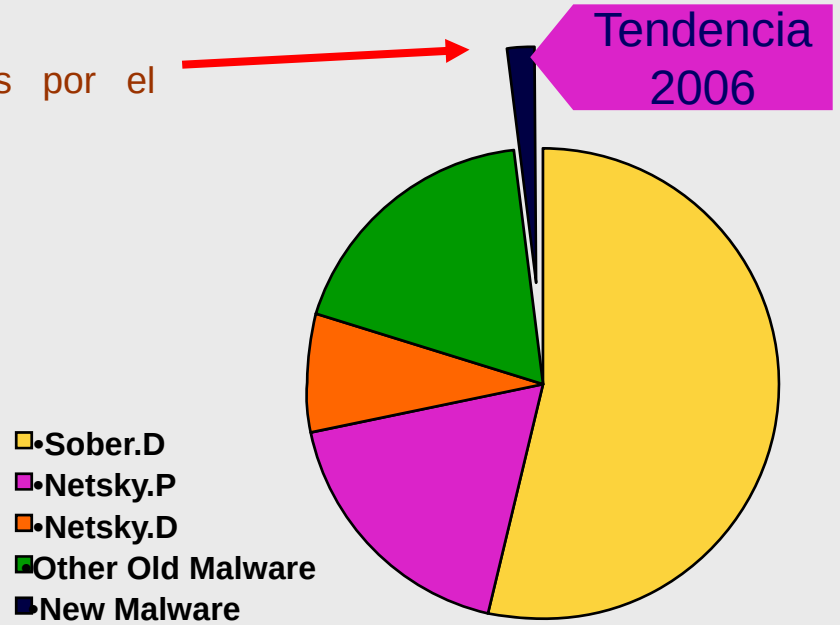
9 de cada 10 ordenados conectados a Internet tienen algún tipo de MALWARE

Hasta 4 saltos para evitar localización.

Software Dañino

- Malware
  - Programa con capacidad SW escrito con intención malicioso que actúa sin permiso del usuario.
  - Virus
    - Programa con capacidad de replicación. Su actividad se manifiesta.
  - Gusanos
    - Programa autocontenido con capacidad de diseminación.
  - **Caballos de Troya**
    - Programa que realiza acciones desconocidas por el usuario o Sistema donde se ejecuta.
    - PUP,s
      - Spyware
      - Admare
  - **Phising y Pharming**
  - Spam
  - Zombies / Botnet

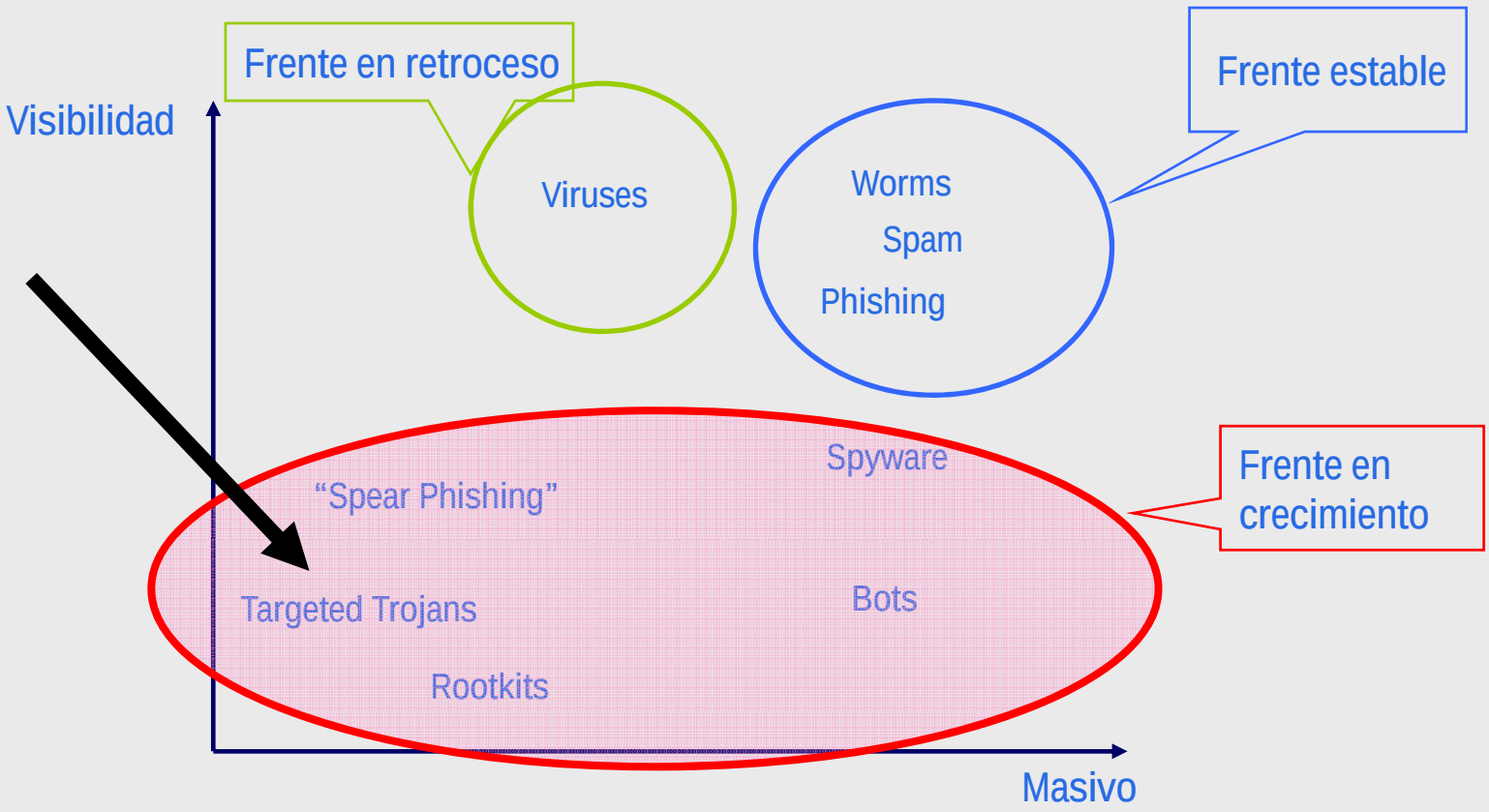




Source: MessageLabs July 2005

Estado actual

- **NUEVO SW DAÑINO** → más peligroso y menos visible.

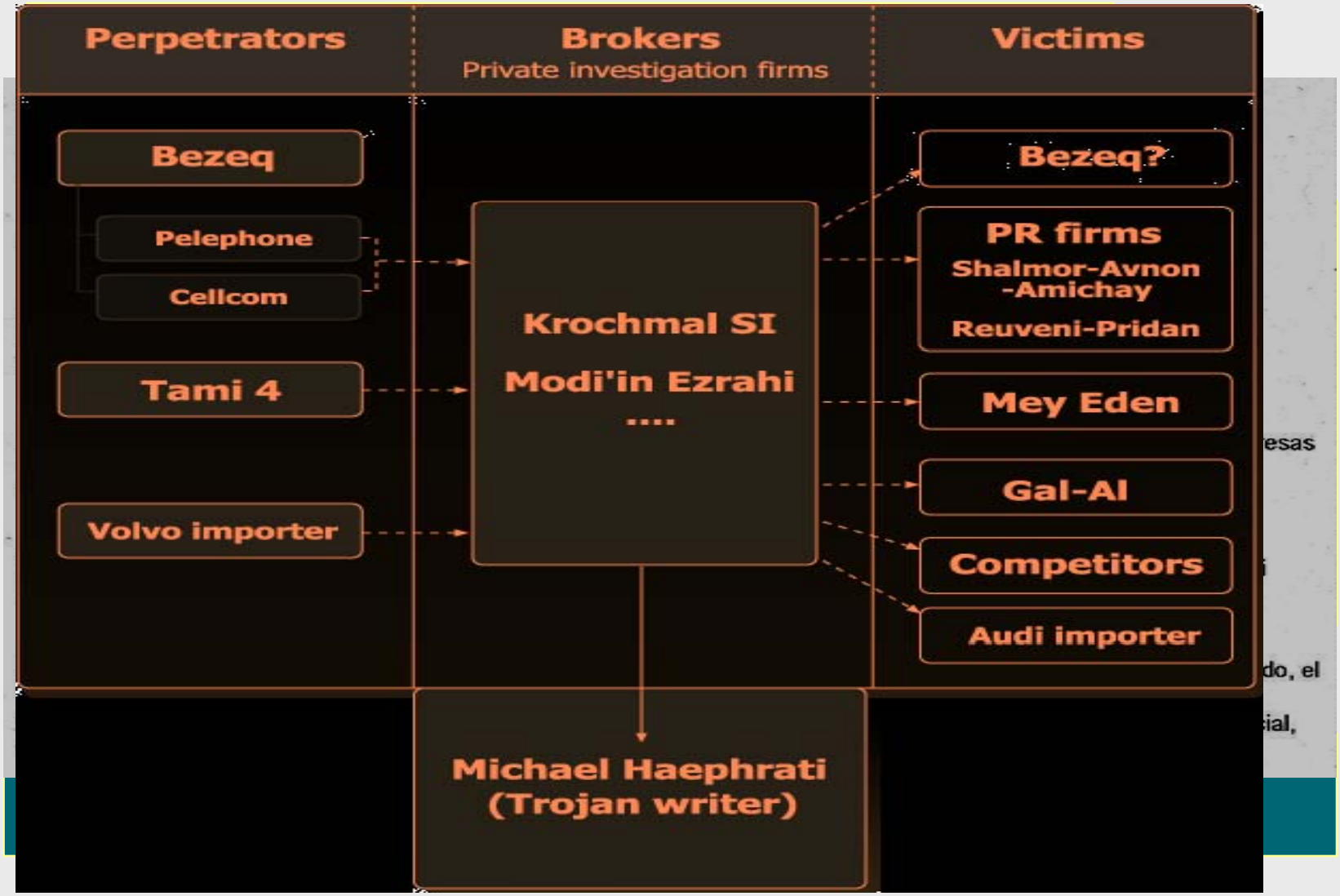


- Spyware -

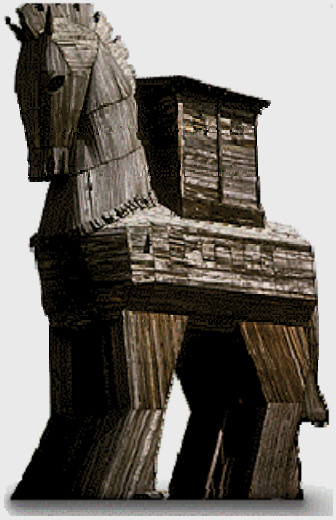
Entre los programas espías se pueden encontrar diversas familias

- Cookies
  - Las “cookies” permiten identificar las áreas de interés y los hábitos de utilización por parte de los usuarios.
- Adware
  - Programas que instalen componentes en el ordenador para registrar la información personal del usuario.
- Monitores del Sistema
  - Programas que capturan todo aquello que el usuario realiza en su ordenador almacenándolo cifrado o enviándolo automáticamente.
- Caballos de Troya
  - Auténtico “malware”: acceso remoto, instalación automática de programas, cifrado de discos, destrucción de archivos, ...

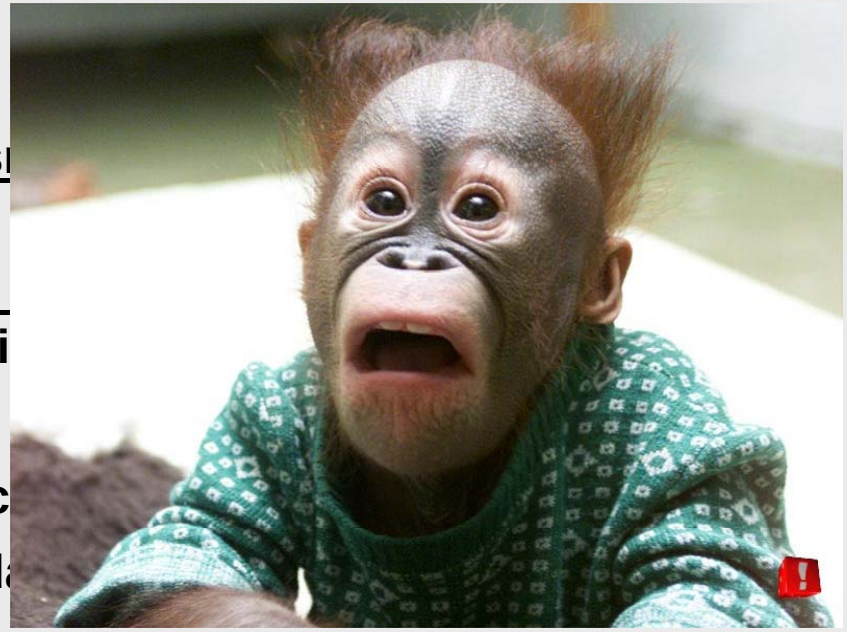
Caballos de Troya / Rootkits …. Caso Israel



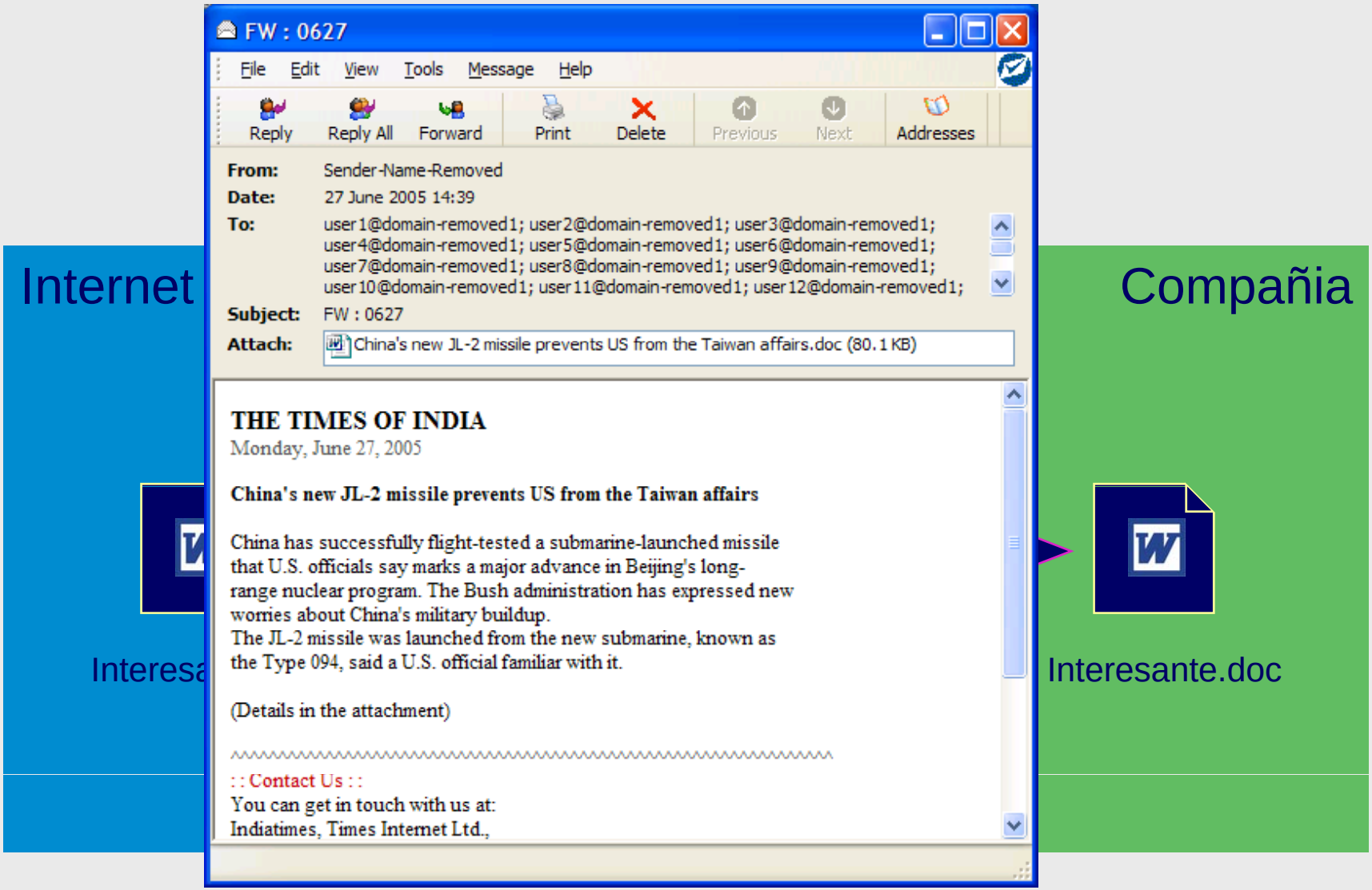
CABALLO DE TROYA



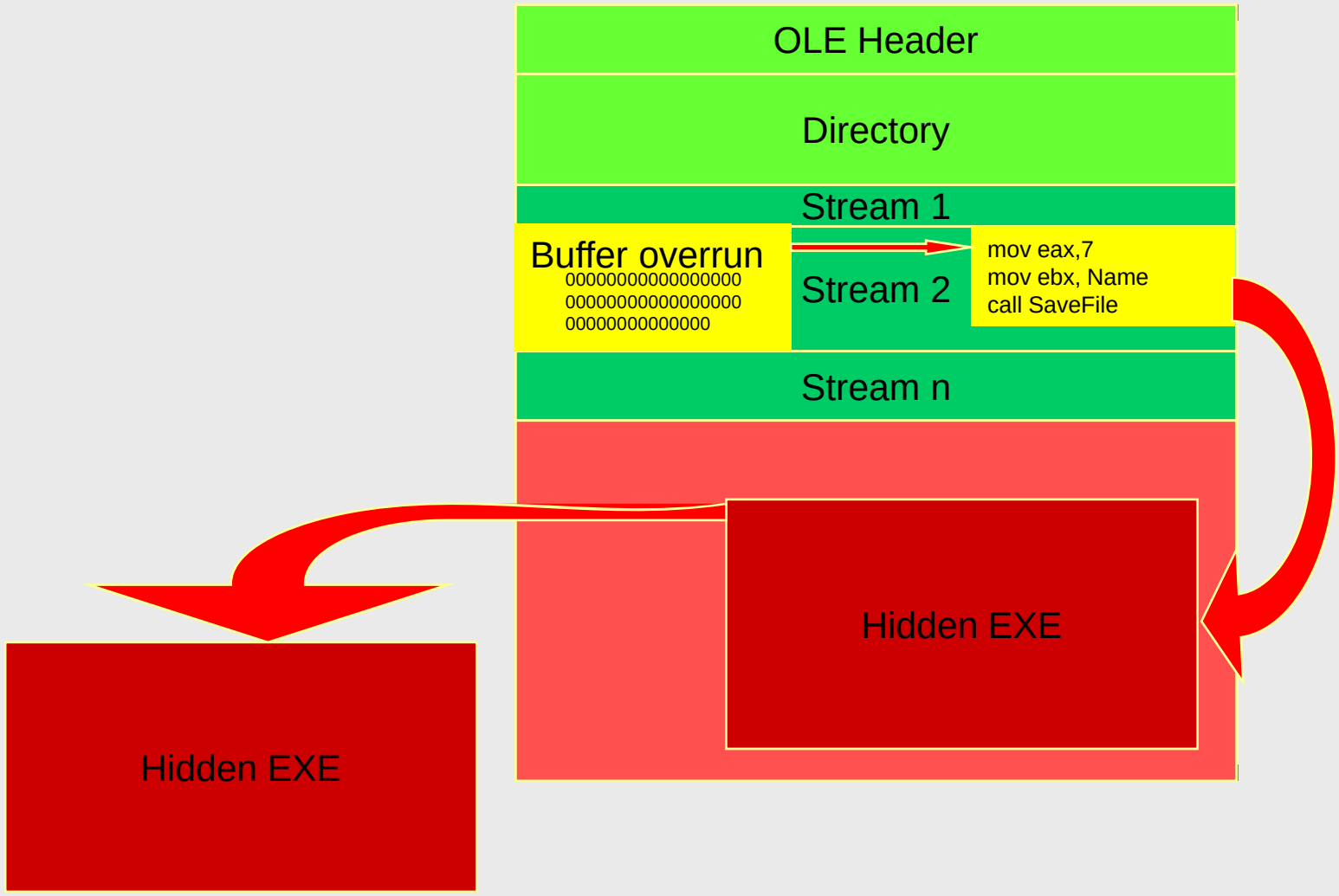
- Un software agresivo. Generalmente atenta contra la confidencialidad de los datos del sistema objetivo
- Se ejecuta en el ordenador agredido.
- Denominaciones:
  - Puertas traseras
  - Root kit
  - Accesos remotos
  - Spyware
- Dispone de un mecanis
  ser detectado
- Utiliza mecanismo para
  transmisión de informaci
- Mecanismo de infección
  - Aplicaciones comerc
  - Instalac. intencionad



Ejemplo de Troyano I (Infección)

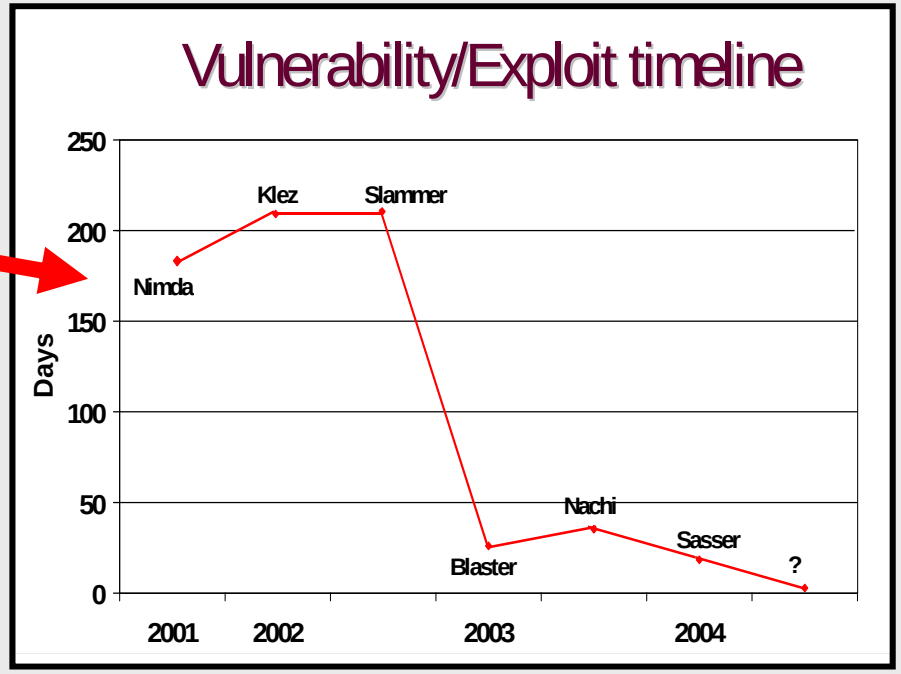


Ejemplo de Troyano II



Ejemplo de troyano (III)

- **Patrón de ataque**
  - Escaso número de objetivos (10-100)
  - Objetivos seleccionados
  - Emplean exploits basados en vulnerabilidades recientes
  - No es detectado por el SW antivirus de los equipos (No dispone de firma)
  - Empleo de mecanismos de cifra resistentes al análisis
  - Permanece sin ser detectado por MESES



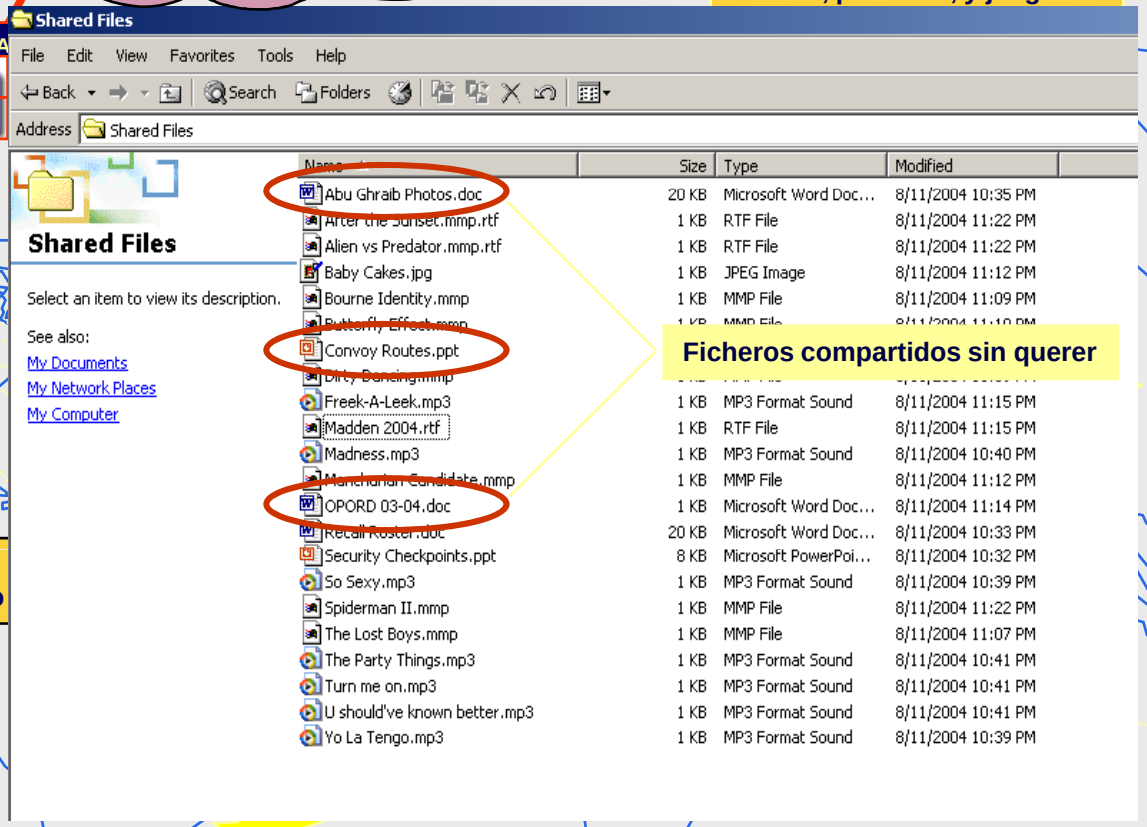
- Análisis detallado de los ficheros del sistema
  - (Mucho tiempo)
- Análisis del tráfico

Programas Potencialmente peligrosos PUP´s

INTERNET

Red P2P empieza a compartir musica, peliculas, y juegos

KAZAA



Ficheros compartidos sin querer

VIRUS

Sitio X

Software busca e identifica Otros usuariosP2P en mundo

Asia

Australia

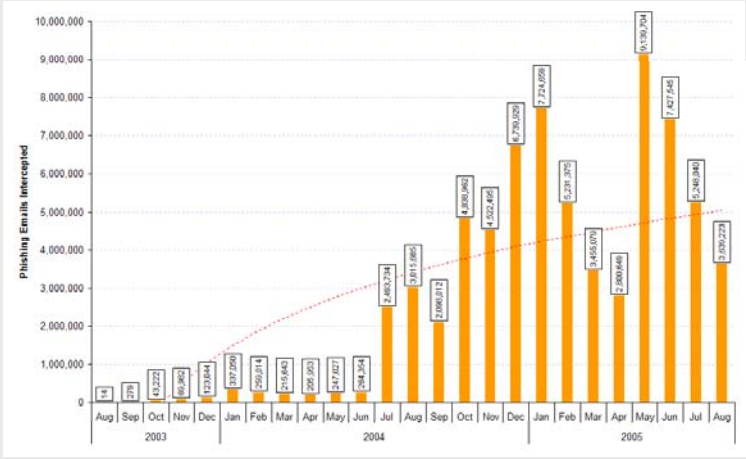
VIRUS

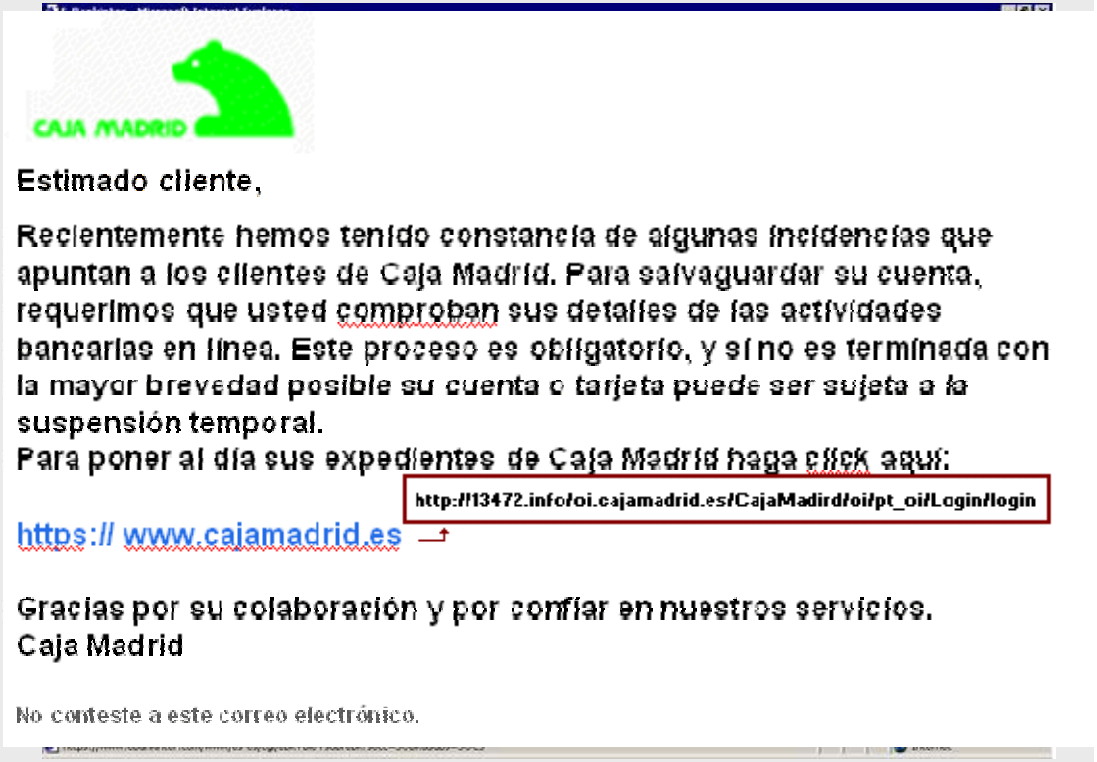
Algunos ficheros contienen virus Y troyanos

La actividad P2P afecta a la organización y al rendimiento del personal
. En peligro información que se encuentre en el equipo.

Phishing y Pharming

- **"Phishing"** es el acto que consiste en recomendar la visita a una página web falsa, haciendo creer al visitante que se encuentra en la página original o copiada
- "**Pharming**" es una nueva amenaza, más sofisticada y peligrosa, que consiste en manipular las direcciones DNS (Domain Name Server) que utiliza el usuario.





Phishing / Tipos de ataque

- **1º NIVEL Tipos de ataque web banca**
  - **Protocolo HTTP es inseguro**
  - **Inyección de código**
- **2º NIVEL Tipos de ataque….. Formulario de firma**

-Troyanización del teclado virtual
  - Manipulación del gestor de teclado virtual

-Captura de coordenadas del teclado virtual
  - Inyección de código que capture clicks de ratón.
  - Ver ejemplo

-Decodificación directa de coordenadas de teclado
  - Implementación pobre.
  - Empleo del propio script de la aplicación bancaria.

Ejemplo Capturas de teclado

Contraseña = "imposible"

```
xterm - Shell No. 2 - Konsole
Session  Edit  View  Bookmarks  Settings  Help
sexy paros # tail /var/log/apache2/access_log
127.0.0.1 - - [21/Mar/2006:19:45:36 +0100] "GET /503.84 HTTP/1.1" 404 262
127.0.0.1 - - [21/Mar/2006:19:45:36 +0100] "GET /667.230 HTTP/1.1" 404 263
127.0.0.1 - - [21/Mar/2006:19:45:37 +0100] "GET /571.357 HTTP/1.1" 404 263
127.0.0.1 - - [21/Mar/2006:19:45:37 +0100] "GET /508.190 HTTP/1.1" 404 263
127.0.0.1 - - [21/Mar/2006:19:45:37 +0100] "GET /624.119 HTTP/1.1" 404 263
127.0.0.1 - - [21/Mar/2006:19:45:38 +0100] "GET /719.198 HTTP/1.1" 404 263
127.0.0.1 - - [21/Mar/2006:19:45:38 +0100] "GET /624.297 HTTP/1.1" 404 263
127.0.0.1 - - [21/Mar/2006:19:45:38 +0100] "GET /660.152 HTTP/1.1" 404 263
127.0.0.1 - - [21/Mar/2006:19:45:39 +0100] "GET /540.57 HTTP/1.1" 404 262
127.0.0.1 - - [21/Mar/2006:19:45:39 +0100] "GET /352.109 HTTP/1.1" 404 263
sexy paros #
```

"GET /352.109"

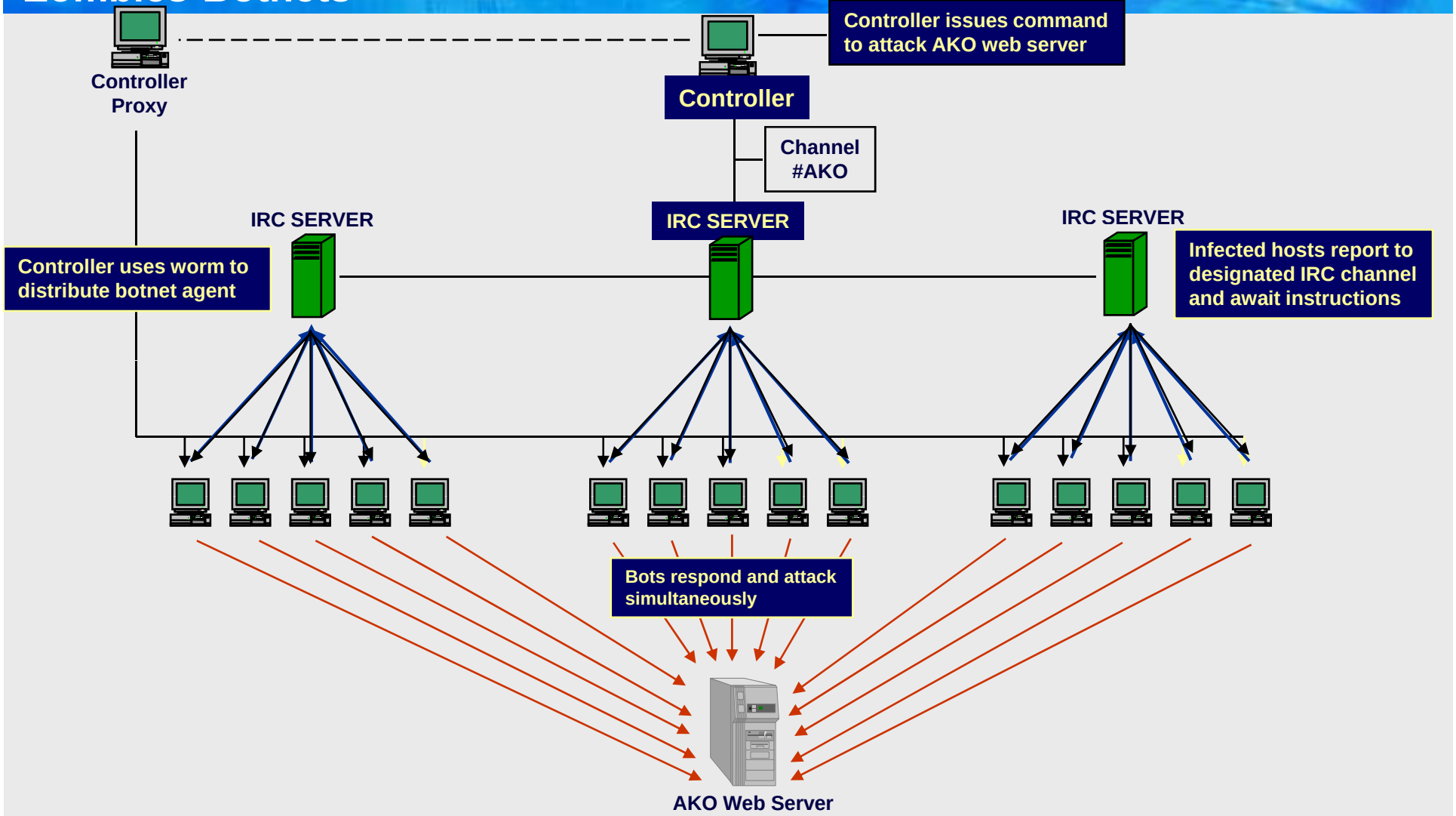
Equivale a la posición x=352 e Y=109.

Zombies-Botnets

"Botnet" es un término utilizado para una colección de robots (software) autónomos que pueden ser controlados remotamente por diversos medios (IRC / P2P) con propósitos maliciosos

- Las máquinas "zombie" se aglutinan en las denominadas "botnets".
- Los sistemas se comprometen utilizando diversas herramientas (gusanos, caballos de troya, puertas traseras, etc…).
- Los zombies pueden escanear su entorno propagándose a través de las vulnerabilidades detectadas (contraseñas débiles, exploits, buffer overflows, etc…).
- La misión de los "botnets" es esencialmente la gestión de los "zombies" creando una infraestructura común de mando y control.
- SPAM / DDOS/ PHISING / ENVIO TROYANOS

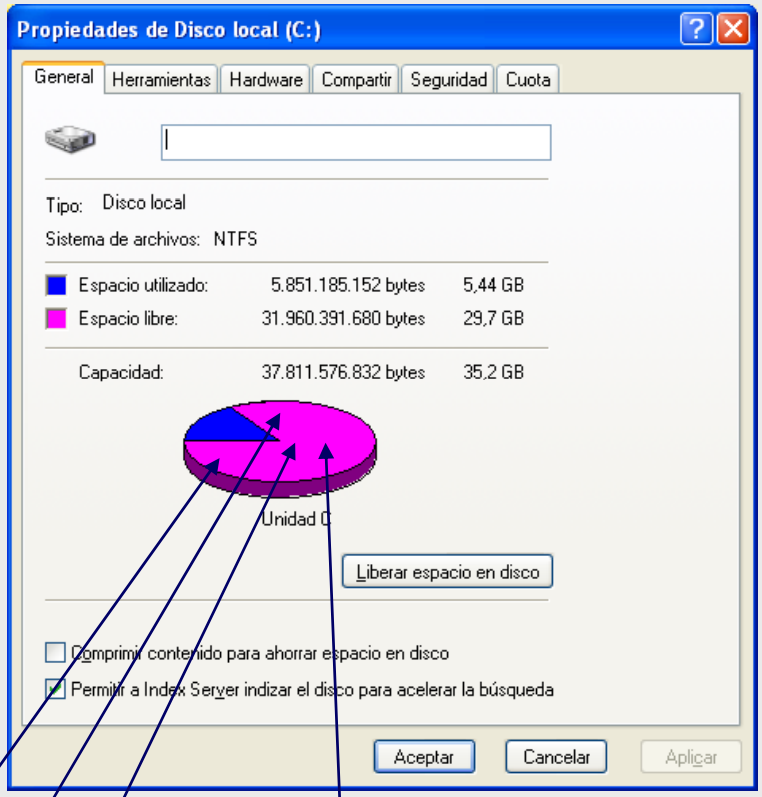
Zombies-Botnets



Ejemplo de ataque de denegación de servicio.

Soportes de Información

En los discos duros de los ordenadores hay enormes cantidades de datos ocultos para los usuarios, pero fácilmente accesibles. Entre estos datos se encuentran archivos que ingenuamente creemos que hemos borrado, claves de acceso, versiones descifradas de archivos confidenciales y todo tipo de rastros sobre la actividad del equipo.



Número de tarjeta de crédito

Copias en legibles de los documentos cifrados

Los registros temporales con datos de clientes

Claves de acceso a sitios seguros

Soportes de información

- OBTENCIÓN DE INFORMACIÓN
  - -Ficheros
    - Metadata
  - -Soportes (Discos duros, disquetes, pen-drives...)
    - Útiles
    - Borrados
    - Tachados
    - Estropeados
    - Rotos

Un estudio revela la importancia de "limpiar" los discos duros antes de deshacerse de ellos

¿Va a deshacerse de su viejo ordenador? Pues tenga cuidado de la información que pueda quedar en su disco duro. Según un estudio realizado por dos estudiantes del prestigioso MIT (*Massachusetts Institute of Technology*), las empresas y los particulares venden o se deshacen con frecuencia de antiguos discos duros con información sensible.

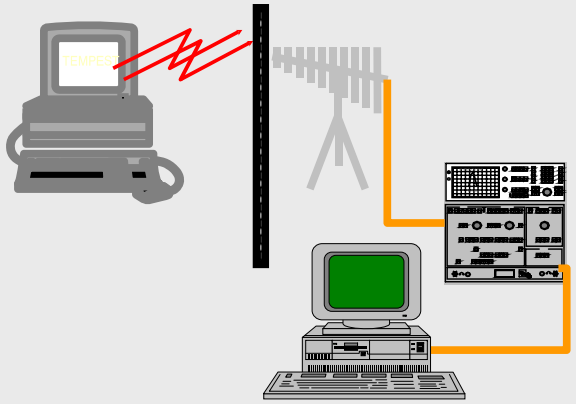
El estudio, denominado "A remembrance of data passed: a study of disk sanitization practices" (Recuerdo de antiguos datos: estudio de las prácticas de saneamiento de discos), analiza un total de 158 unidades de disco duro adquiridas a través de la web de subastas de eBay, en tiendas informáticas, empresas e intercambios. El informe destaca que el 74% de los discos contenían antiguos datos que se podían recuperar y leer. El 17% contenían sistemas operativos totalmente instalados y operativos con datos de usuario para cuya recuperación no era necesario mucho esfuerzo. Un 57% de los discos habían sido formateados, pero todavía contenían datos antiguos recuperables. Sólo el 12% habían sido adecuadamente limpiados (o saneados) antes de ponerlos a la venta, y 29 de los 158 discos analizados directamente no funcionaban.

Entre la información recuperada de estos discos había registros financieros empresariales, datos personales, información médica, cartas de amor y gigabytes de e-mail personales y pornografía.

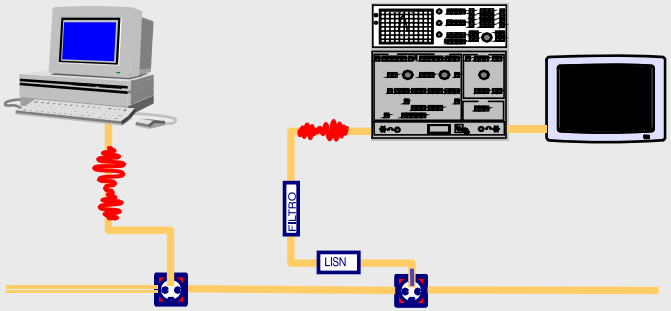
Aceptar Cancelar

Amenaza TEMPEST

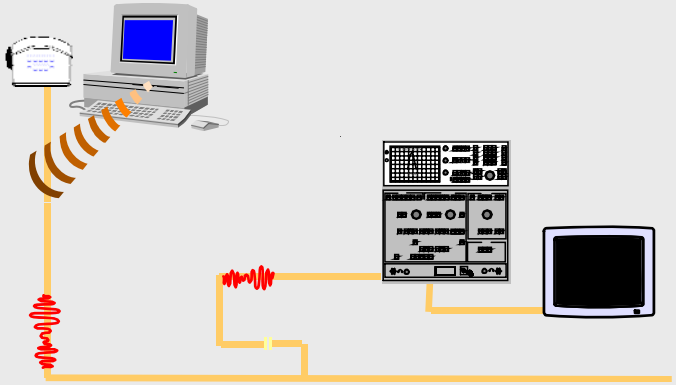
Señal radiada



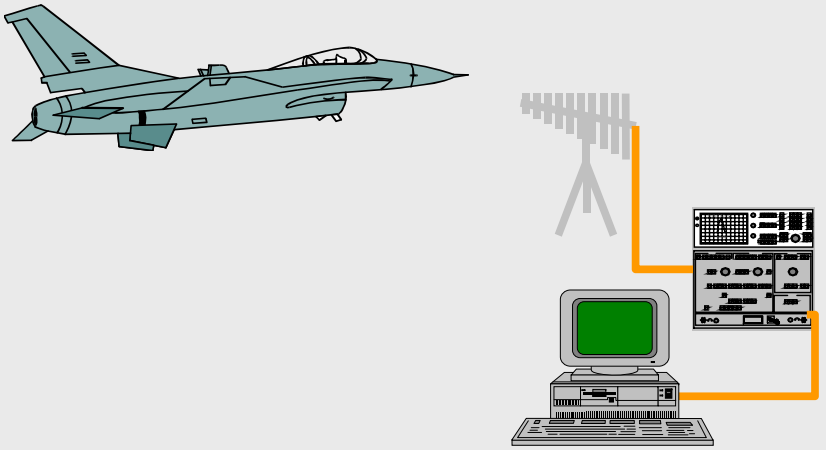
Señal inducida. Alimentación



Señal inducida. Línea de comunicaciones



Acoplamiento en transmisores



Futuras amenazas

- Aumento de vulnerabilidades 0-day.
- Explotación de Redes P2P.
- Incremento de programas PuP (Potencial Unwanted Programs) Spyware – Adware.
- Incremento de RootKits con keyloggers.
- Incremento de Phising.
- Incremento de Vishing.
- Incremento de Smishing.
- Ataques sobre plataformas 64bits.
- Incremento de malware sobre la telefonía movil.
- Incremento de malware sobre VoIP.

CONTRAMEDIDAS

Algunos Consejos – Código Malicioso (I) - Usuarios

- **TENER ACTUALIZADO EL SISTEMA OPERATIVO CON LOS ULTIMOS PARCHES.**
- **TENER INSTALADO Y ACTIVADO UN ANTIVIRUS.**
- **TENER INSTALADO/CONFIGURADO UN CORTAFUEGOS.**
- **TENER INSTALADO UN PROGRAMA ANTI-SPYWARE.**

http://www.spywarewarrior.com/rogue_anti-spyware.htm

- **TENER PROTEGIDA LA PAGINA INICIAL DEL NAVEGADOR.**
- **TENER PROTEGIDO EL FICHERO HOST.**

Algunos Consejos – Código Malicioso (II)

✔ **USAR PARA LA NAVEGACIÓN EN INTERNET UN USUARIO QUE NO TENGA PRIVILEGIOS EN EL SISTEMA.**

× **REALIZAR COPIAS DE SEGURIDAD PERIODICAS.**

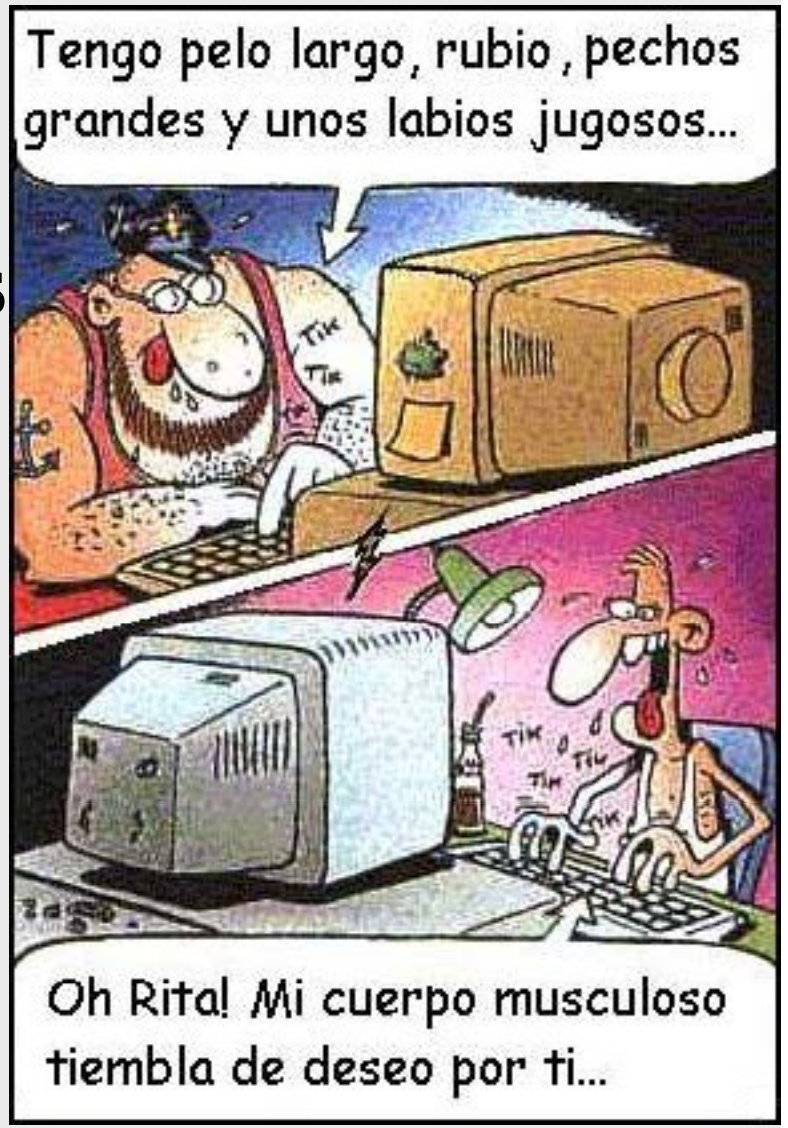
× **NO ABRIR NINGÚN MENSAJE RECIBIDO A TRAVÉS DEL CORREO ELECTRÓNICO DE FUENTES DESCONOCIDAS O DUDOSAS.**

× **ANALIZAR TODOS LOS ARCHIVOS, INCLUSO LOS COMPRIMIDOS.**

× **NUNCA ABRIR DOCUMENTOS ANEXADOS DE FUENTES DESCONOCIDAS, GUARDAR EN UN CARPETA TEMPORAL Y ANALIZAR. NO BAJAR NADA DE SITIOS WEB POCO CONFIABLES.**

Reflexión

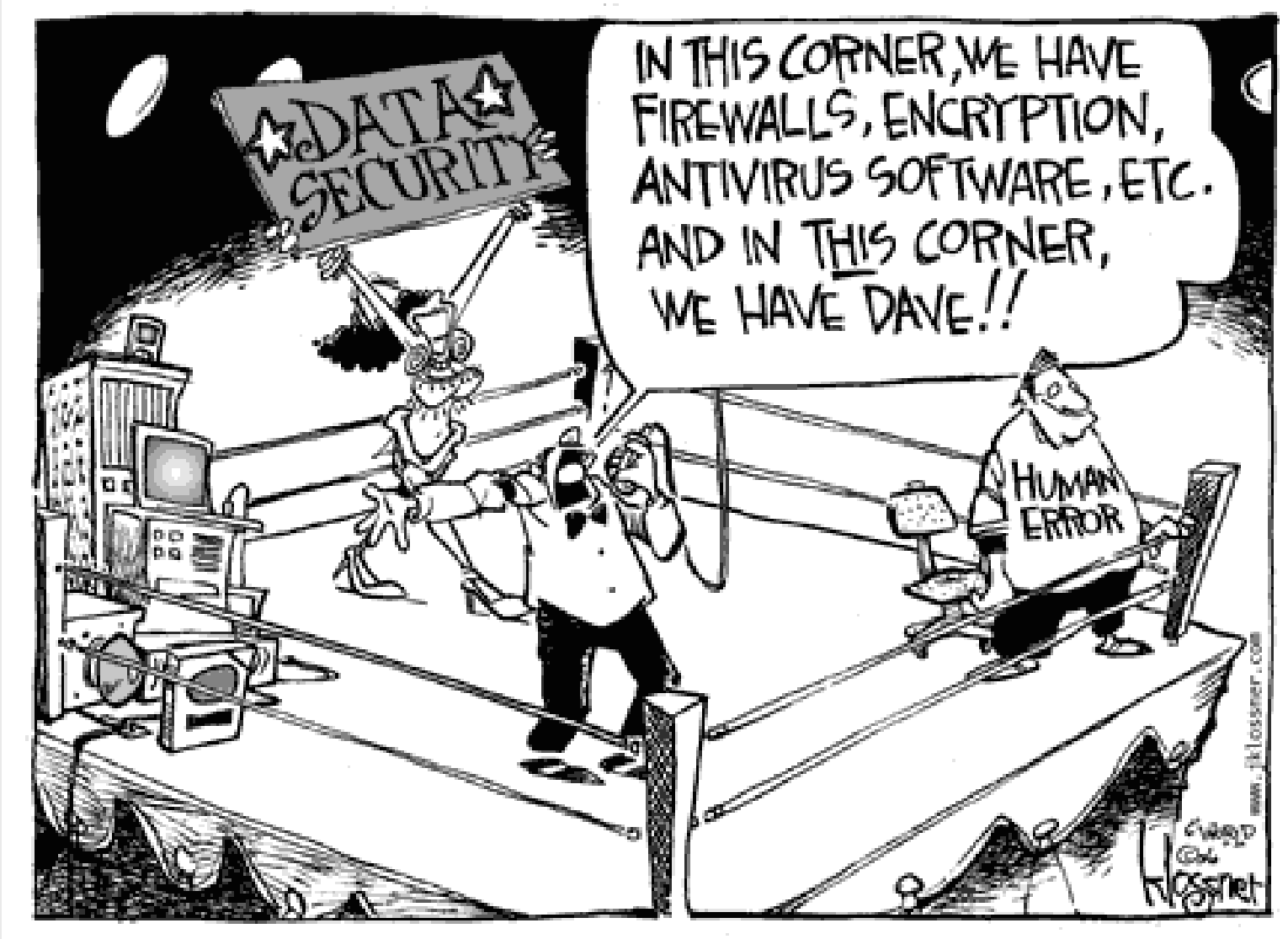
- ¿DEBO DE CONFIAR EN EL REMITENTE?
- ¿PUEDO CONFIAR EN ARCHIVOS ADJUNTOS?
- ¿REALMENTE ES UN FICHERO DE TEXTO (.txt) O UN FICHERO CON TEXTO ENRIQUECIDO (.rtf)?
- ¿PUEDO CONFIAR EN MENSAJES CON FORMATO (.html)?
- ¿DEBO DE CONFIAR EN LA PAGINA WEB VISITADA?



Algunos Consejos – Organización

- MEDIDAS DE SEGURIDAD PERIMETRALES.
- SEPARACIÓN FÍSICA DE TODAS LAS REDES.
- ESTRICTA POLÍTICA ANTIVIRUS. CONTROL DE TODOS LOS FLUJOS DE ENTRADA DE INFORMACIÓN A LA ORGANIZACIÓN.
- ESTRICTA POLÍTICA DE SEGURIDAD DE LA ORGANIZACIÓN. ¿QUÉ, CÓMO, DÓNDE?.
- FORMACIÓN CONTINUA DE LOS RESPONSABLES DE SEGURIDAD.
- AUDITORÍAS EXTERNAS.
- SEGURIDAD ACTIVA.

Usuarios Internos



Conclusiones

- Amenazas cada vez más complejas y difíciles de detectar.
- Formación de personal para luchar contra:
  - Ingenuidad.
  - Ignorancia de buenas prácticas.
  - Falta de concienciación.
- Hay que tomar conciencia de los riesgos.
  - Medidas Legislativas, Procedimentales, Organizativas y Técnicas.
- Herramientas de Seguridad (Medidas Técnicas).
- Productos Certificados.
- Inspecciones de Seguridad
- Gestión de incidentes

Información Adicional

http://www.centrocriptologiconacional.es

http://www.oc.ccn.cni.es

http://www.ccn-cert.cni.es

formacion.ccn@cni.es

acreditacion.ccn@cni.es

ccn@cni.es

ccn-cert@cni.es

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Muchas Gracias