UNIVERSIDAD PONTIFICIA
ICAI ICADE
COMILLAS
MADRID

Seguridad Informática:

Capítulo 9: Virus y antivirus

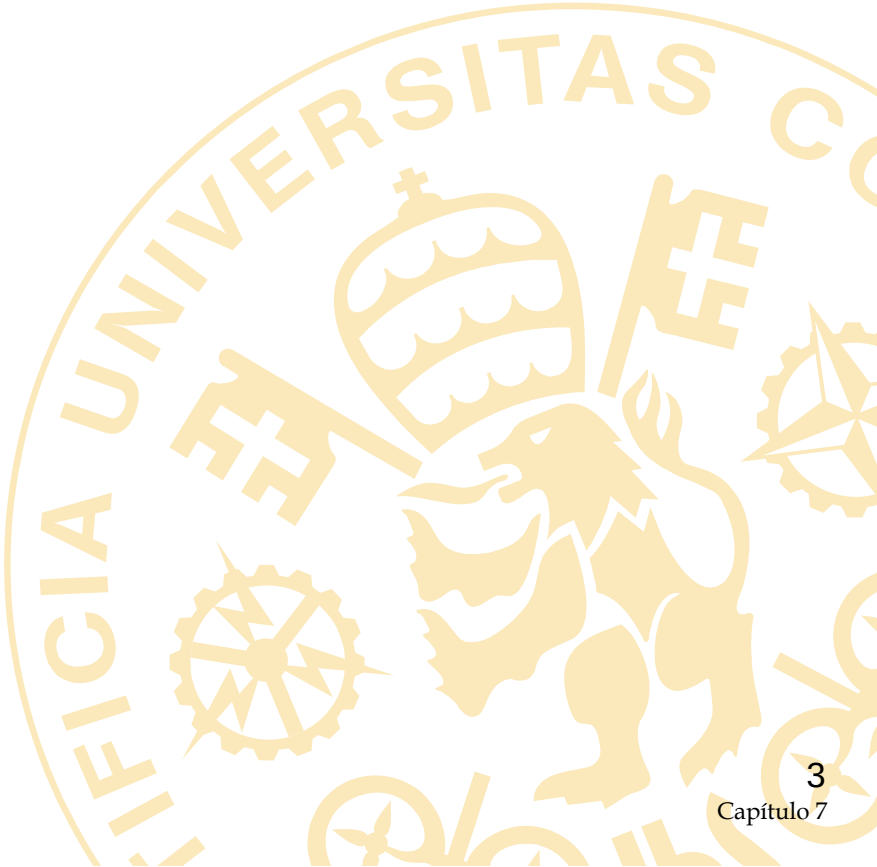
Titulación: Ingeniero en Informática.
Curso 5º - Cuatrimestral (2006-2007)

Javier Jarauta Sánchez
José María Sierra
Rafael Palacios Hielscher

Contenido

- Introducción
- Definición y clasificación de virus
- Funcionamiento general de los virus
- Tipos de virus
- Protección contra virus
- Ejemplos de virus
- Resumen

Introducción



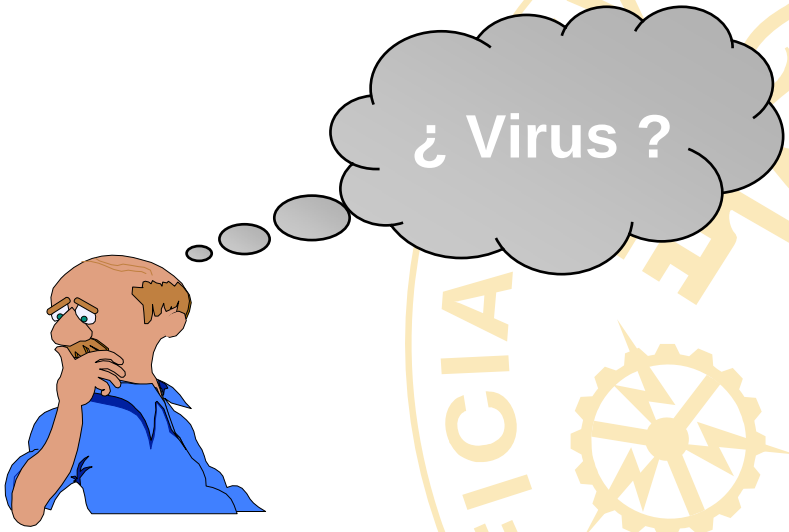
Introducción

Desconocimiento

+

mala información

= **Confusión**



Introducción histórica

- Década de los 60: Programadores de Bell diseñan un juego llamado Core War (guerras de núcleo)
- 1983: Fred Cohen acuña el nombre de virus (programas que se reproducen a si mismos)
- 1985: Aparecen los primeros troyanos disfrazados de gráficos y juegos
- 1986: Aparece Brain (Pakistaní) y se extiende por todo el mundo (sector de arranque de discos 5,25")
- 1987: Stoned (sector de arranque)
- 1987: Viernes-13 o Jerusalem (primer v.residente)
- 1988: 2 de Noviembre. Gusano de Internet. Colapso en 3 horas mediante e-mail
- 199x: Auge de los virus de propagación por Internet
- 200x: Spyware y Phishing

Volumen de virus (McAfee, mayo 2007)

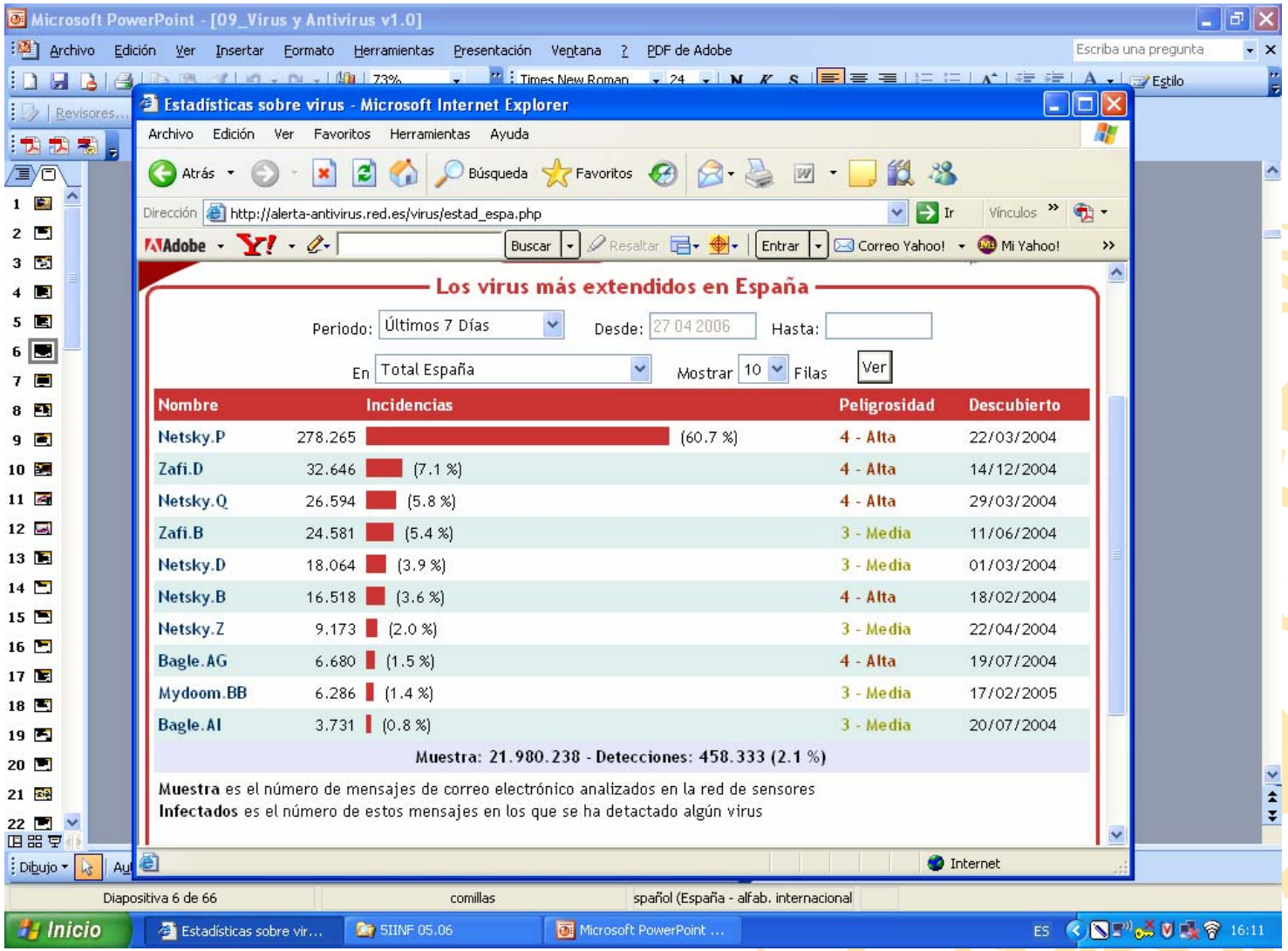
- Actualmente hay más de 180.000 amenazas
- Approximately 150 to 200 viruses, Trojans, and other threats emerge every day
- During December 2005 there were 7.6 million **new** zombies (source TechNewsWorld)
  - 250,000 new infected computers per day

Incidencias de virus en España 2005

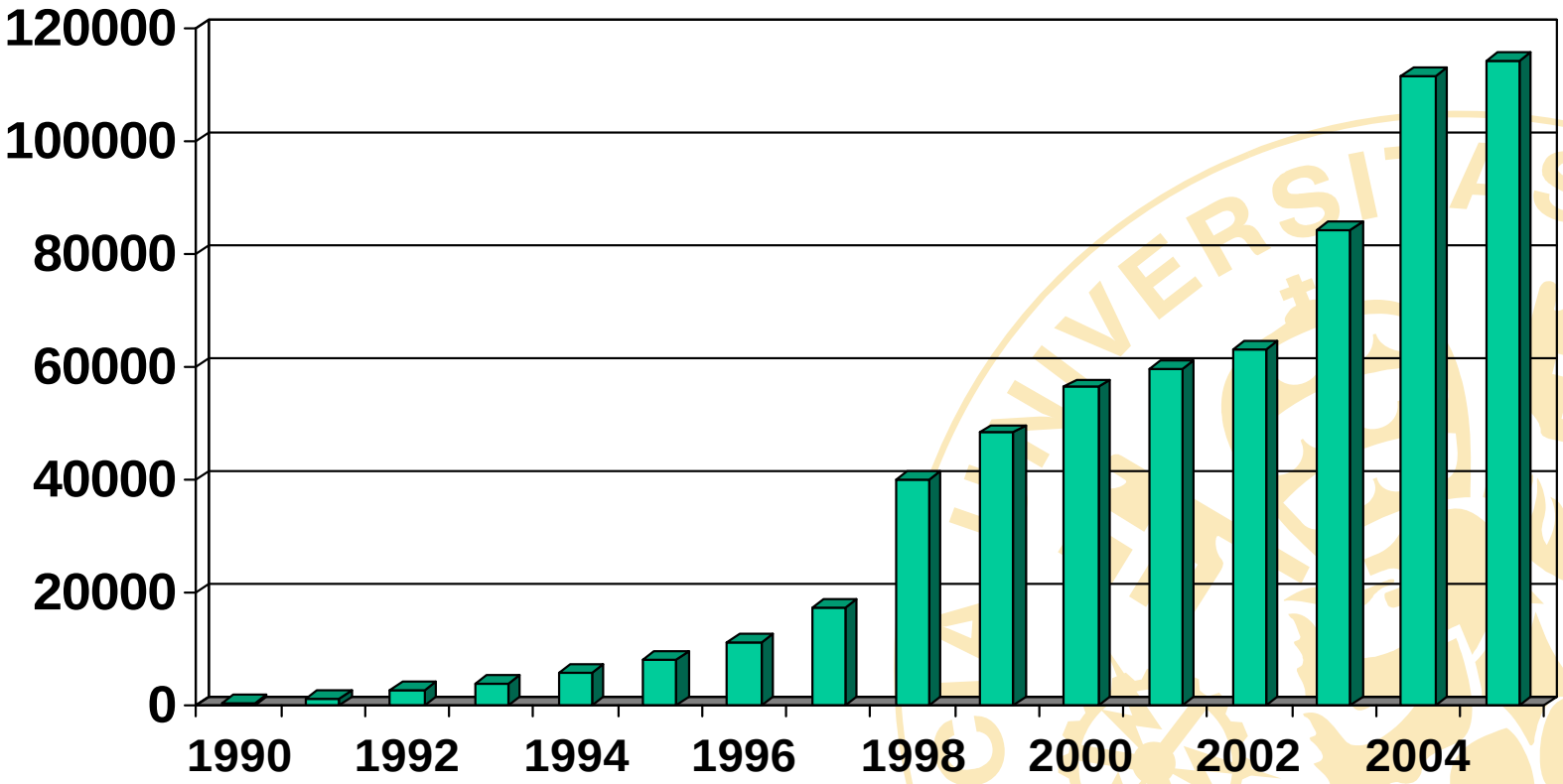
Nombre	Incidencias	Peligro	Fecha
Netsky.P	74.175.814 (41.7%)	Alta	22/03/2004
Netsky.B	23.903.954 (13.4%)	Alta	18/02/2004
Netsky.Q	14.552.235 (8.2%)	Alta	29/03/2004
Zafi.B	14.289.770 (8%)	Alta	11/06/2004
Mydoom	7.252.897(4.1%)	Media	27/01/2004
Bagle.AB	6.649.870(3.7%)	Alta	29/04/2004

En una muestra de 1.123 Millones de email analizados
el 15,8% tenían virus

Incidencia virus en España última semana



Totales Malware = 114.175 Feb 2005



Fuente: McAfee's VirusScan statistics

Evolución en el tiempo . . .

Marzo 2005

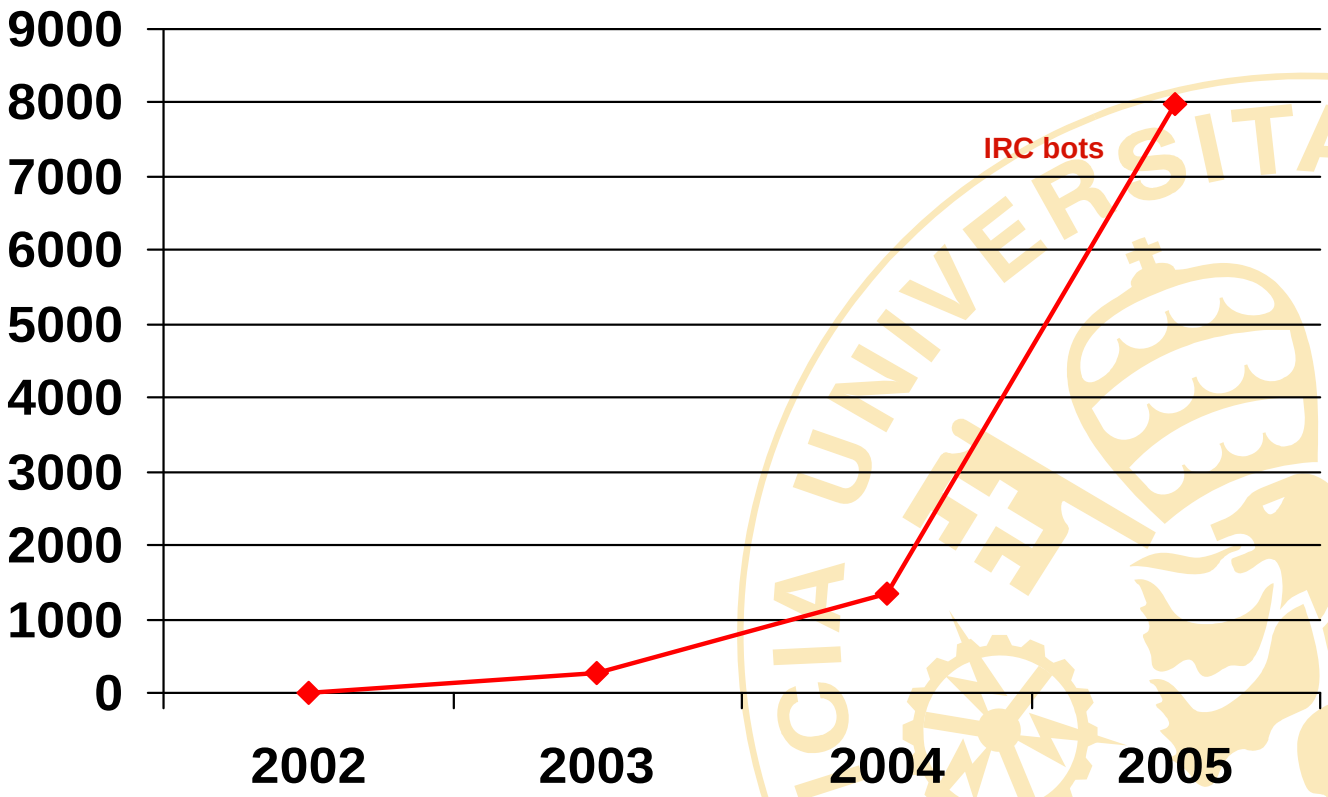
- 850 Virus Sector de Arranque
- 40400 Virus DOS
- 8250 Win32 y gusanos
- 8600 macro viruses
- 18700 Troyanos
- 7900 BAT, scripts, HTML, script exploits
- 350 Virus y troyanos Linux
- 9 Amenazas PDA
- 50 Virus y troyanos MacOS
- 2500 Drivers de aplicación, jokes y dialers

Agosto 2005

- 850 Virus Sector de Arranque
- 44500 DOS viruses
- **15100** (7100 Win32/gusanos y **7900** BOTs)
- 8625 Virus de Macro
- **21200** Troyanos
- **8500** BAT, scripts, HTML, script exploits
- 380 Virus y troyanos Linux
- 13 Amenazas PDA
- 50 Virus y troyanos MacOS
- 3000 Drivers de aplicación, jokes y dialers

Fuente: McAfee's VirusScan statistics

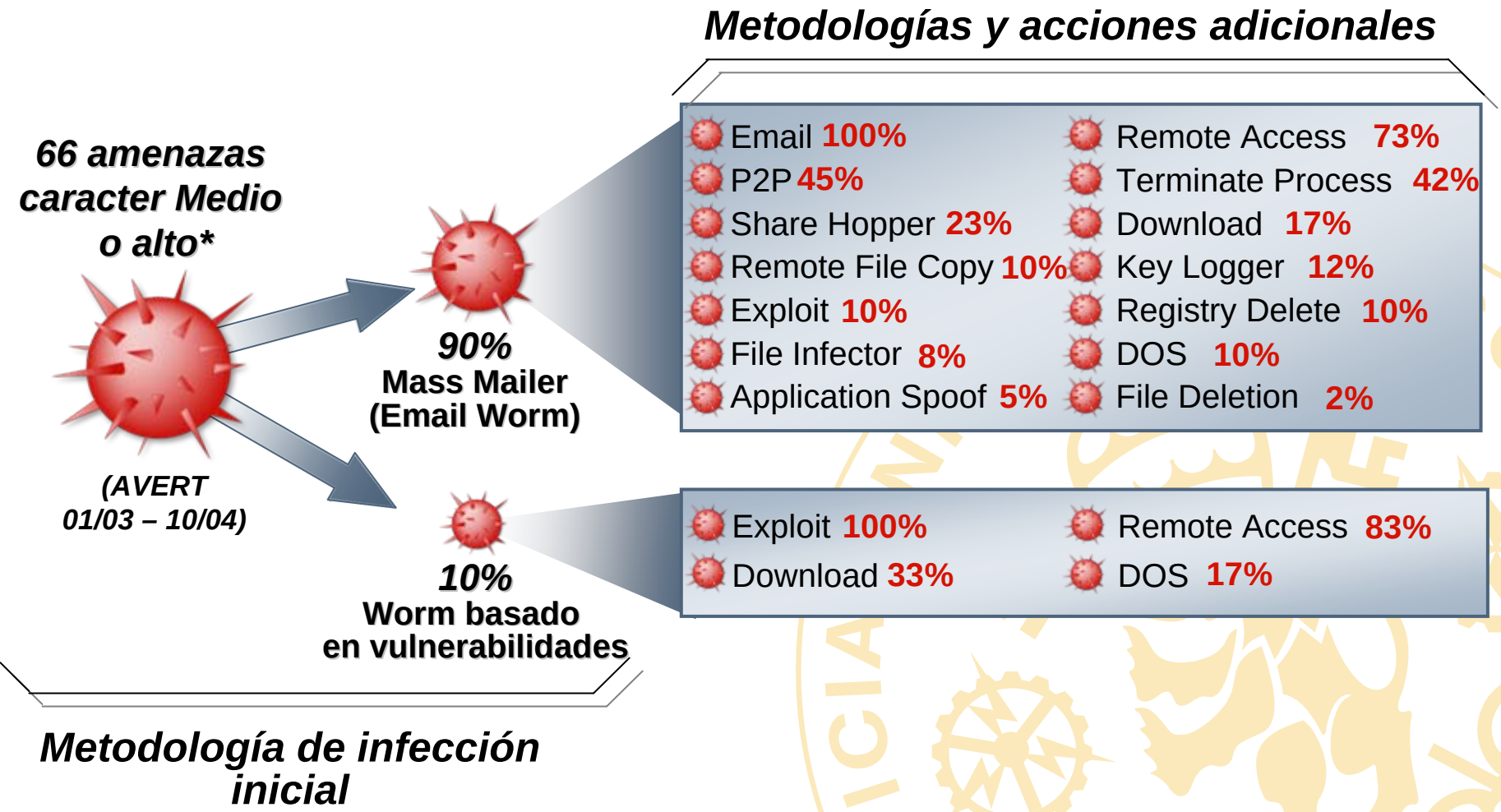
IRC malware (bots)



Fuente: McAfee's VirusScan statistics

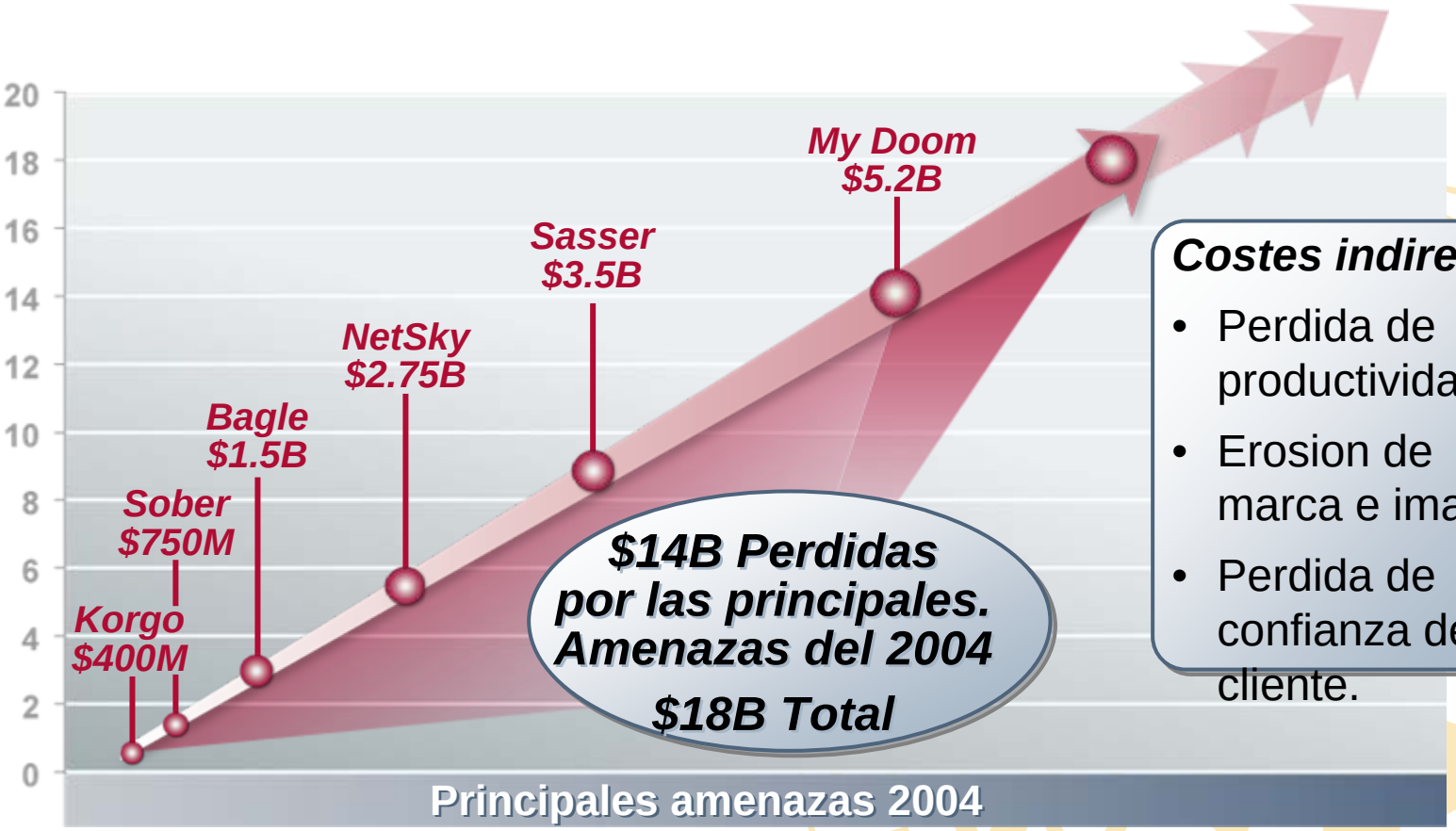
Servidores de malware...

Panorama actual



Fuente: McAfee's VirusScan statistics

Impacto en el negocio por amenazas



Costes indirectos

- Perdida de productividad
- Erosion de marca e imagen
- Perdida de confianza del cliente.

Source: Computer Economics 12/04

Desde la vulnerabilidad a la amenaza

Fuente: McAfee's VirusScan statistics

Informe de sophos trimestre 1,2007

- En el último año se ha duplicado el número de nuevas amenazas malware.
- En el primer trimestre de 2007 se detectaron 24.000 malware, frente a 10.000 en el primer trimestre de 2006.
- La web (navegador) es el principal medio de transmisión. Hay más conciencia de seguridad en el correo.
- De enero a marzo de 2007 una media de 5000 nuevas páginas web con capacidad de infección (el 70% son páginas legítimas donde el atacante ha tomado el control).

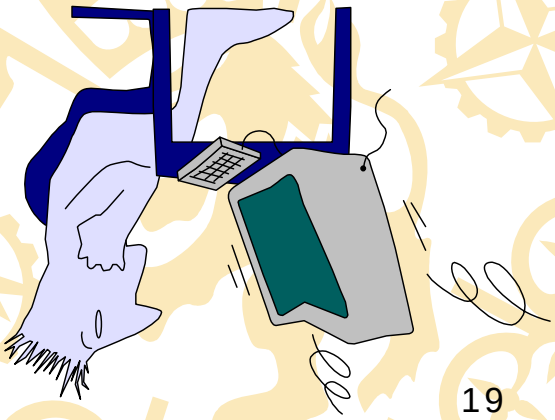
Definición y clasificación de virus

Definición y propiedades

- Un virus es una secuencia de instrucciones (programa)
  - De código máquina compilado, o
  - De código fuente interpretado
- Es capaz de
  - Realizar copias reiteradas de si mismo (propagarse)
  - Añadir su código al de otros programas (infectar)
- Infecta a programas normales a través de
  - La ejecución involuntaria y parasitaria de un programa previamente infectado

Definición y propiedades

- Intentan controlar el entorno en el que actúan para
  - Poder propagarse
  - Permanecer oculto al usuario
- Por este motivo suelen ser residentes en memoria, aunque existen tipos de virus que no son residentes
- Utilizan técnicas de ocultación
- Sus especificaciones dificultan el funcionamiento normal del ordenador al que infectan
- Generalmente provocan daños



Definición y propiedades

- Toman el nombre de los virus biológicos y se establecen ciertas analogías:
  - Virus biológico entra en el cuerpo e infecta las células. El virus informático entra en el ordenador e infecta los archivos.
  - Ambos virus se reproducen y se propagan dentro del sistema. También se propagan a otros sistemas transmitiendo la infección.
  - Los virus biológicos son microorganismos y los virus informáticos son micro-programas.
  - Los primeros programas para eliminar virus se llamaron vacunas, aunque ahora se llaman antivirus.

Definiciones de programas peligrosos

- **Virus**: Programa difícil de detectar que se replica y extiende. En determinados momento puede causar daños importantes
- **Worm** (gusano): programa que se replica y extiende. No necesita infectar otros programas para extenderse, normalmente se extiende por la red produciendo mucho tráfico.
- **Trojans** (caballos de Troya): programa que aparenta ser inofensivo mientras realiza su tarea.

Definiciones de mensajes de correo

- **Hoaxes** (trampas): no son virus, son falsos mensajes que causan alarma y desconcierto. En algunos casos pueden engañar al usuario para modificar parámetros del sistema y tener efectos parecidos a los de un virus.
- **Spam**: mensajes de correo no solicitado. No suelen ser dañinos sino que causan pérdida de tiempo y sobrecargan la red.
- **Phishing**: técnica moderna de engañar a los usuarios para conseguir información personal.

Clasificación

- Los virus se pueden clasificar por varios criterios:
  - Técnicas utilizadas
  - Dónde se esconden
  - Tipo de archivos que infectan
  - Tipo de daños que causan
  - Tipo de plataforma que atacan
  - Mecanismo de propagación
  - etc.

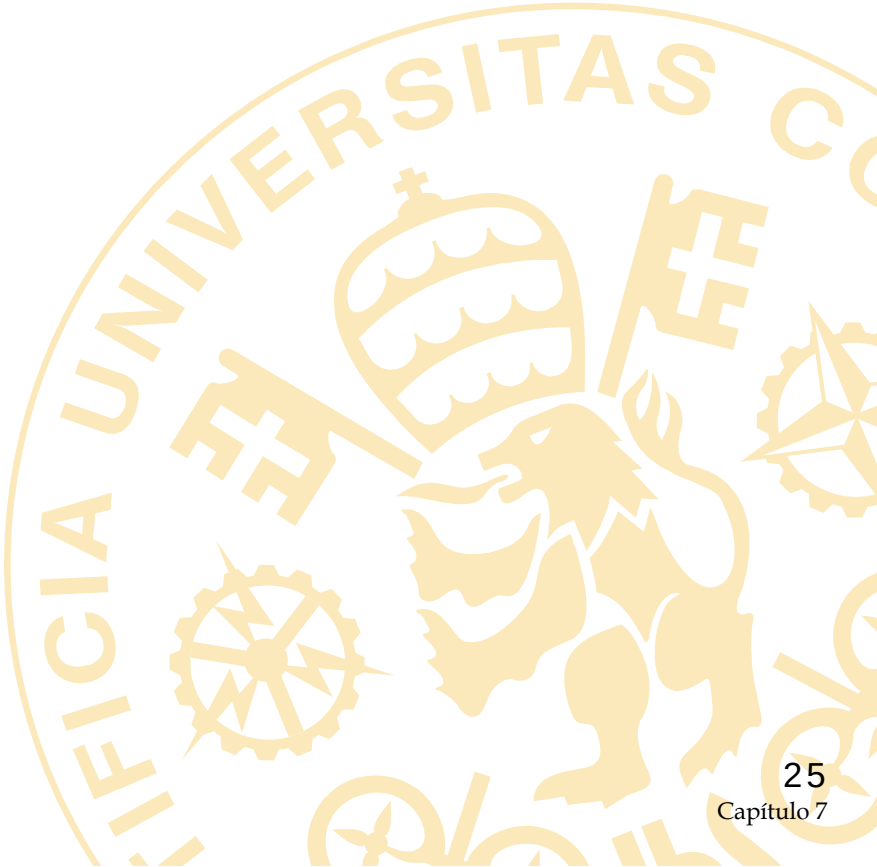
Clasificación

- Lo más extendido es clasificarlos atendiendo fundamentalmente al lenguaje de programación
  - W32 Viruses targetted at all 32-bit versions of Windows (all versions from Windows 95 on).
  - VBS Viruses written in Visual Basic Script.
  - WM, W95, W97M, W2KM: Word macro viruses
  - AM, A97M, A2KM: Access macro virus
  - OM, O97M, O2KM: Office macro virus
  - JS Attacks written in JavaScript.
  - Worm
  - Trojan

Clasificación

TrendMicro

- ActiveX Control
- Backdoor
- Batch File
- Boot
- DOS
- Elf Executable
- File Infector
- Html
- IRC Script
- Java Applet
- JavaScript
- Joke
- Macro
- Not a Virus
- Others
- Shell Script
- Trojan
- VBScript
- Visio 5
- VXD
- Worm



Clasificación

- De cada virus suelen aparecer variantes a los pocos días (sufijos .A, .B,...)

top virus threats

Risk	Threat	Discovered	Protection
4	W32.Netsky.D@mm	March 1, 2004	March 1, 2004
4	W32.Netsky.B@mm	February 18, 2004	February 18, 2004
3	W32.Netsky.P@mm	March 21, 2004	March 22, 2004
3	W32.Beagle.M@mm	March 13, 2004	March 13, 2004
3	W32.Netsky.K@mm	March 8, 2004	March 8, 2004
3	W32.Beagle.J@mm	March 2, 2004	March 2, 2004
3	W32.Beagle.E@mm	February 28, 2004	February 28, 2004
3	W32.Netsky.C@mm	February 24, 2004	February 25, 2004
3	W32.Welchia.B.Worm	February 11, 2004	February 11, 2004
3	W32.Mydoom.A@mm	January 26, 2004	January 26, 2004

Symantec marzo/2004

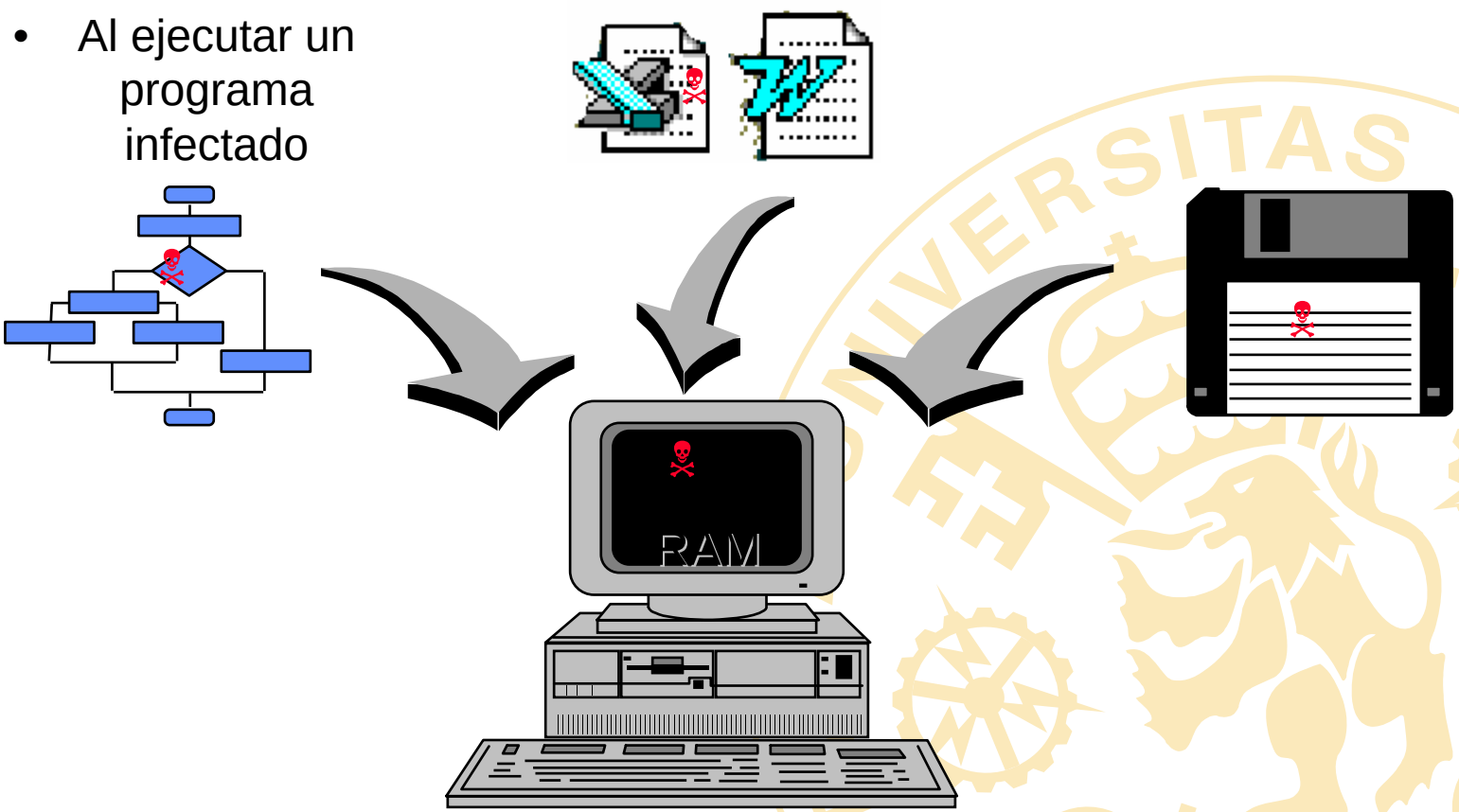
Funcionamiento general de los virus

Ciclo de vida de un virus

Infección Inicial

- Al abrir un documento infectado

- Al ejecutar un programa infectado



Medios de contagio

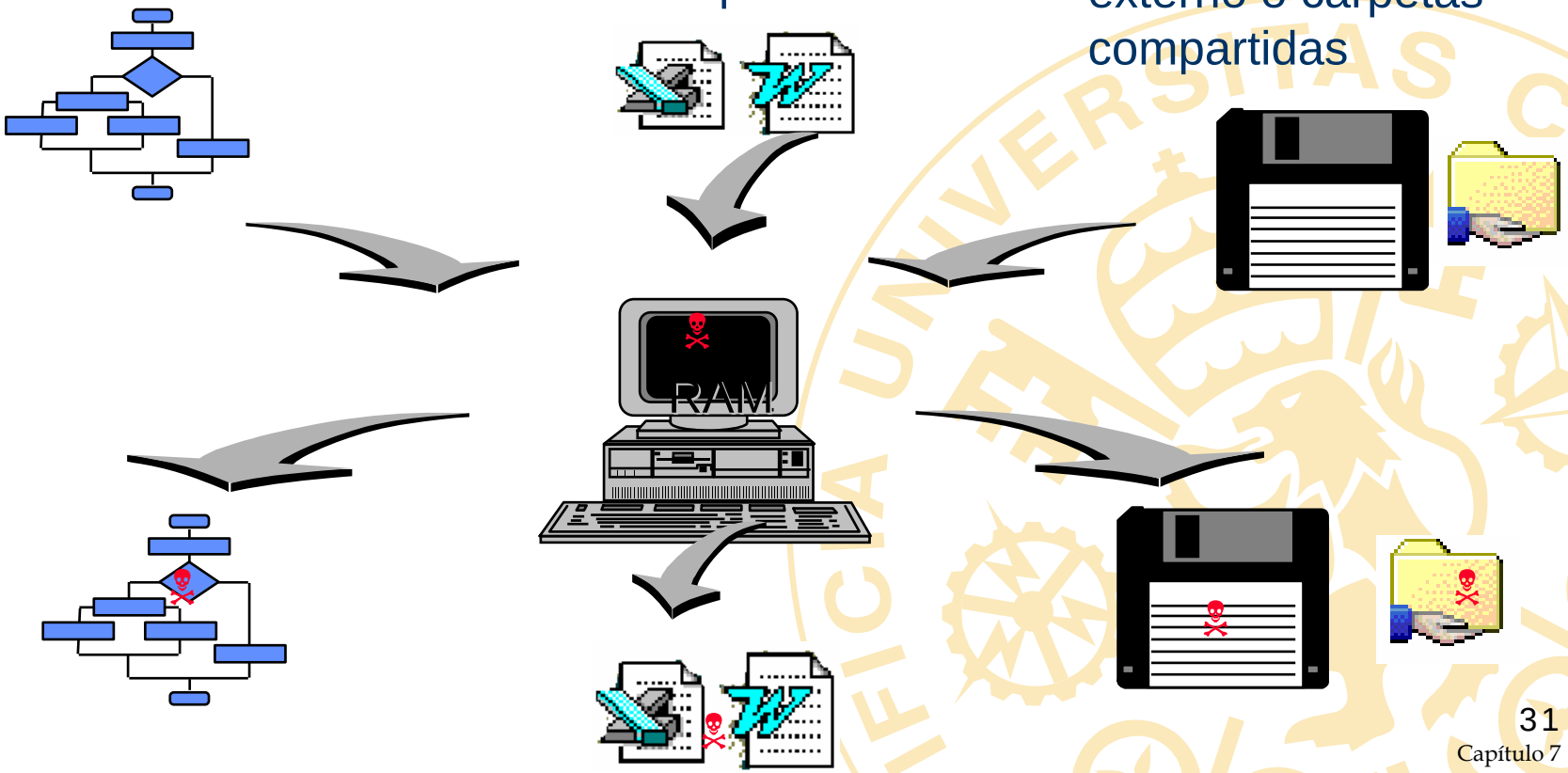
- Intercambio de programas
- Circulación de disquetes, CDs, Flash USB
- Download de ficheros (FTP, HTTP)
- Agujeros de seguridad
- Otras redes públicas y correo electrónico (attachments)
- Revistas en o con disquete o CD-ROM
- Marketing en disquete o CD-ROM

Propagación e infecciones sucesivas

Al ejecutar un programa limpio

Al abrir o salvar un documento limpio

Acceso a dispositivos de almacenamiento externo o carpetas compartidas



Técnicas de ocultación

- Procedimientos que utilizan los virus para no ser detectados por
- Los usuarios
- Los programas anti-virus
- Hacen uso de ellos cuando se están propagando
- Básicamente utilizan las siguientes técnicas
- Capturar las llamadas a interrupciones del sistema operativo
- Cifrar su código
- Utilizar “motores de mutación” para cambiar de aspecto alterando su estructura de programa en cada infección
- Matan el proceso anti-virus

Técnicas de ocultación

- **Stealth**: Esconder los signos visibles de un infección que podría delatar la presencia (tamaño de ficheros)
- **Tunneling**: Contra antivirus residentes. Obtienen direcciones de memoria originales de los servicios para utilizarlos sin ser interferidos.
- **Auto-cifrado**: Se cifran cada vez que infectan un fichero, luego cambian totalmente de aspecto
- **Polimorfismo**: Se cifran cada vez con un modo de cifrado diferente. Son muy sofisticados
- **Armouring**: Técnicas para evitar ser examinados (acorazados)

Síntomas de infección

- Anomalías en el dispositivo de video/ratón
- Aumento de la carga de CPU
- Aumento del tráfico de red
- Accesos inesperados a dispositivos de almacenamiento
- Reducción significativa de la memoria y espacio en disco
- Desaparecen inesperadamente ficheros de datos y programas
- Variaciones en la configuración del equipo
- Mensajes de error no usuales
- Errores al leer, ejecutar o copiar ficheros

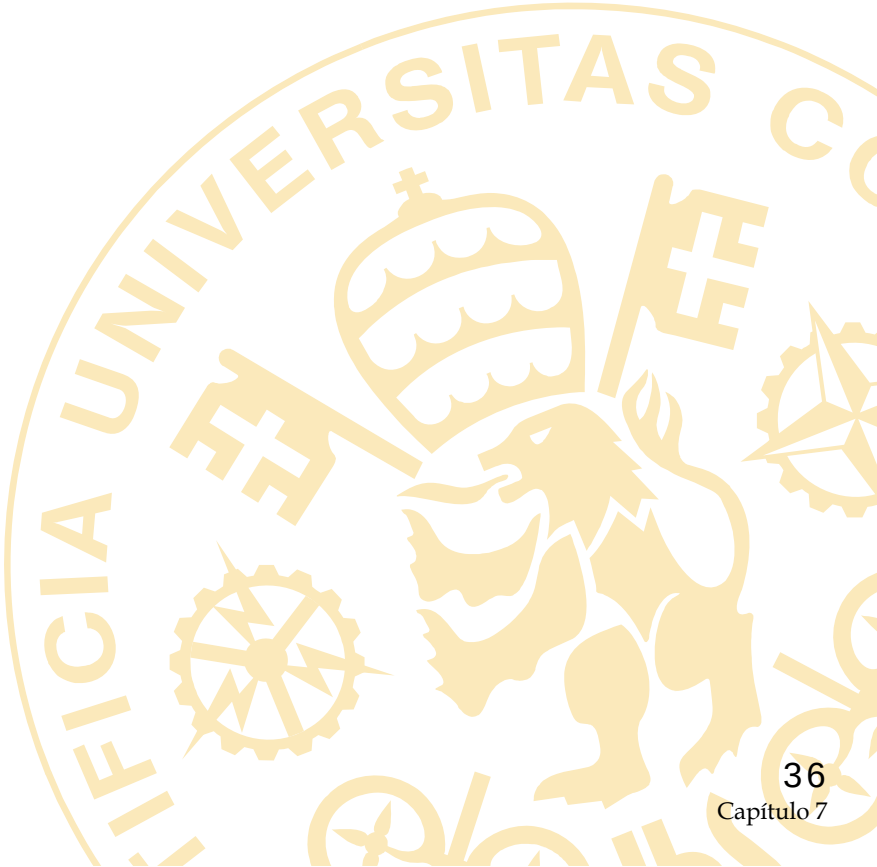
Resumen

- 1.- Un virus es un programa, en código máquina compilado, o en código fuente interpretado que
  - Realiza copias reiteradas de si mismo (se propaga)
  - Añade su código al de otros programas (infecta)

- 2.- La infección se produce si
  - Ejecuto en mi ordenador un programa que ya está infectado
  - Enciendo el ordenador con un disquete infectado en la disquetera
  - Abro un documento infectado
  - Recibo un correo (con ciertos programas de correo)
  - Accedo a una página web maliciosa (con ciertos navegadores)

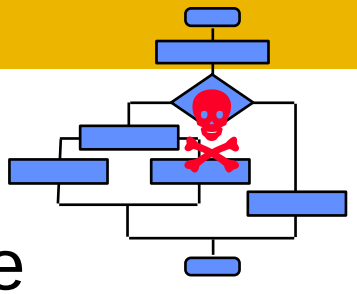
- 3.- Si un equipo está infectado puede propagar el virus si
  - Ejecuto un programa limpio
  - Leo o escribo en un disquete, CD, FlashUSB
  - Abro un documento limpio.
  - Comparto una unidad de red
  - El virus (worm en este caso) se propaga sólo por la red

Tipos de virus

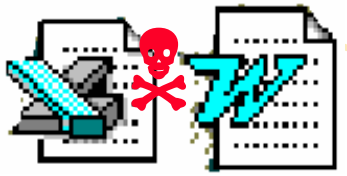


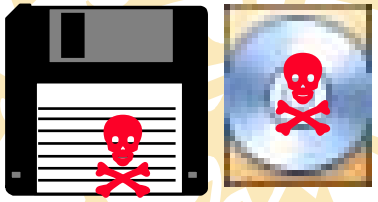
Tipos de virus

Índice



- Virus de fichero ejecutable
- Virus de macro
- Virus de sector de arranque
- Virus de Internet
- Técnica de phishing





Tipos de virus

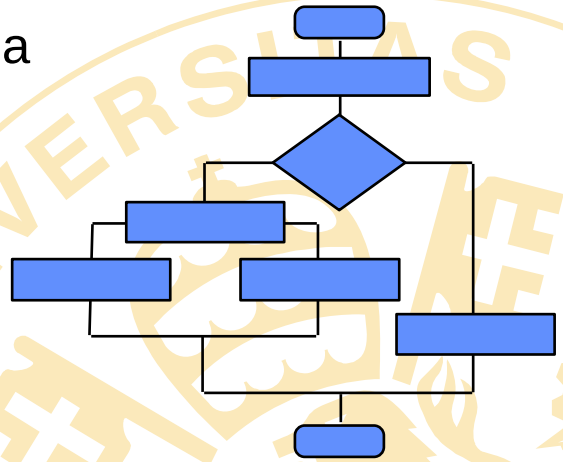
- En función de las “intenciones” del virus
  - Benignos
  - Malignos

- ¿Puede un programa ser benigno si... ?
  - Reduce el tamaño operativo de la memoria RAM
  - Reduce la velocidad de proceso
  - Aumenta el tiempo de respuesta del ordenador
  - Reduce el espacio en disco

¡No existe virus benigno!

Virus de fichero ejecutable (1)

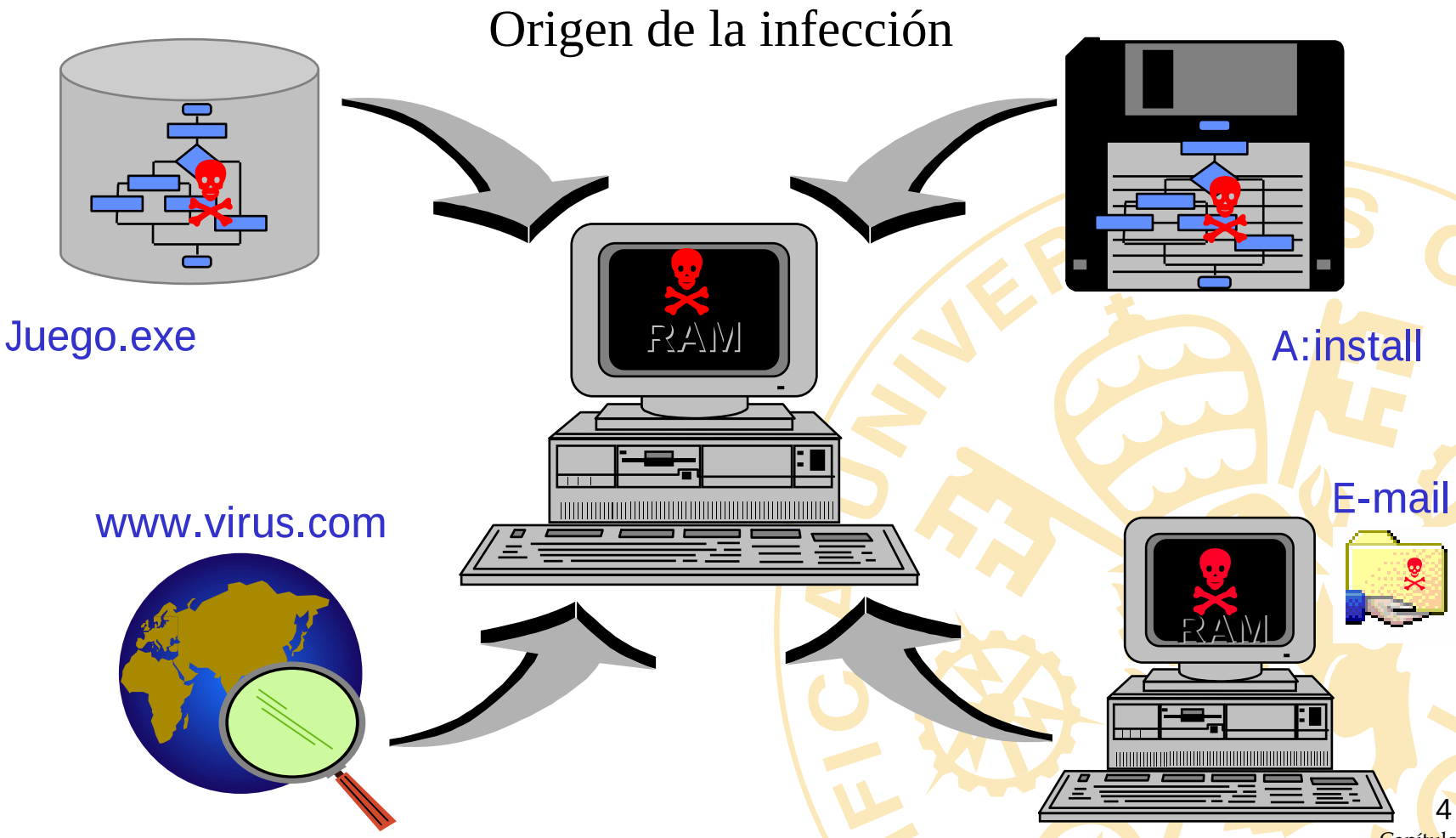
- Fichero ejecutable es un archivo que contiene sentencias de un lenguaje cualquiera de programación compiladas en código máquina
- Es dependiente del S.O. En el que se compila



- Tipos de ficheros ejecutables
  - Directos : *.EXE, *.COM
  - Ampliaciones : *.OVR, *.OVL
  - Drivers : *.DLL, *.SYS
  - Auto-ejecutables / empaquetados : *.ARJ, *.ARC, *.ZIP, *.RAM

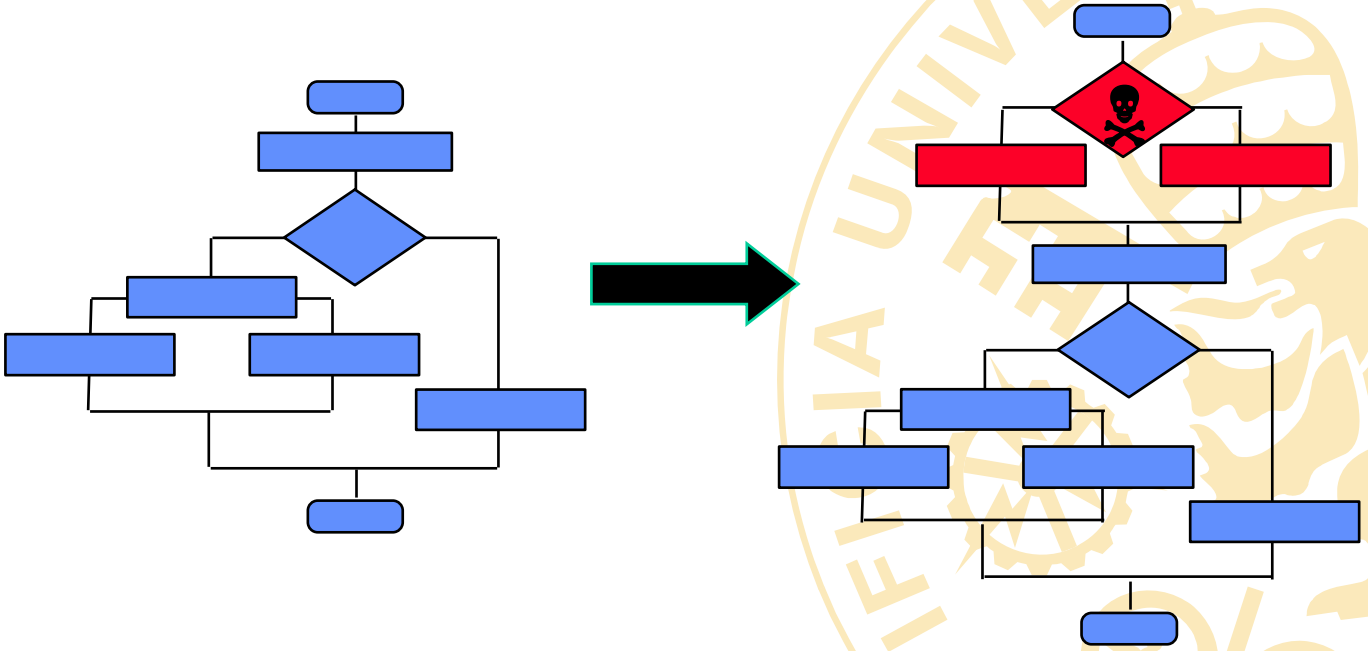
- Ejecuto un programa ➔ el código del virus tiene oportunidad de cargarse en el sistema

Virus de fichero ejecutable (2)



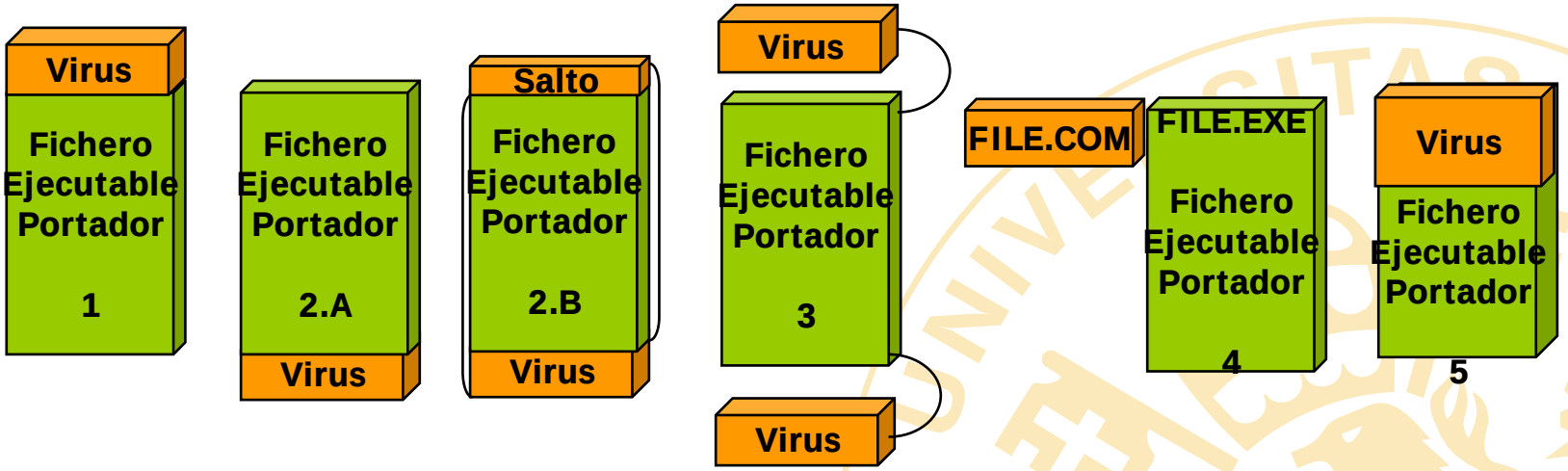
Virus de fichero ejecutable (3)

- Es capaz de modificar la estructura de un fichero ejecutable
- Utiliza el fichero ejecutable como portador
- Consigue así poder ejecutarse de forma desapercibida y parasitaria



Virus de fichero ejecutable (4)

- Técnicas básicas de infección



1.- Pre inserción

2.A- Post inserción pura

2.B.- Post inserción con salto

3.- Recubrimiento

4.- Suplantación COM, EXE

5.- Sobreescritura

Virus de fichero ejecutable (5)

Impacto en el sistema

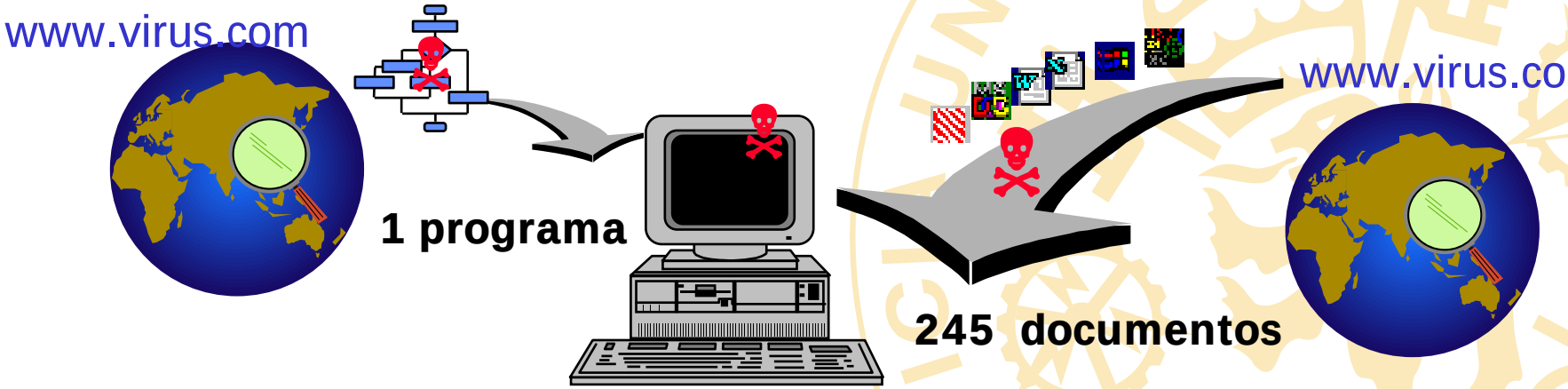
- En el ordenador
  - Disminuye la memoria RAM disponible
  - Reduce la velocidad de proceso
  - Aumenta el tiempo de respuesta

- En el fichero que infecta
  - Aumenta en tamaño del fichero **(engorda el fichero)**
  - El tiempo que tarda en empezar a ejecutarse es mayor
  - Si el virus no está bien programado el fichero puede dejar de funcionar correctamente

Virus de macro (1)

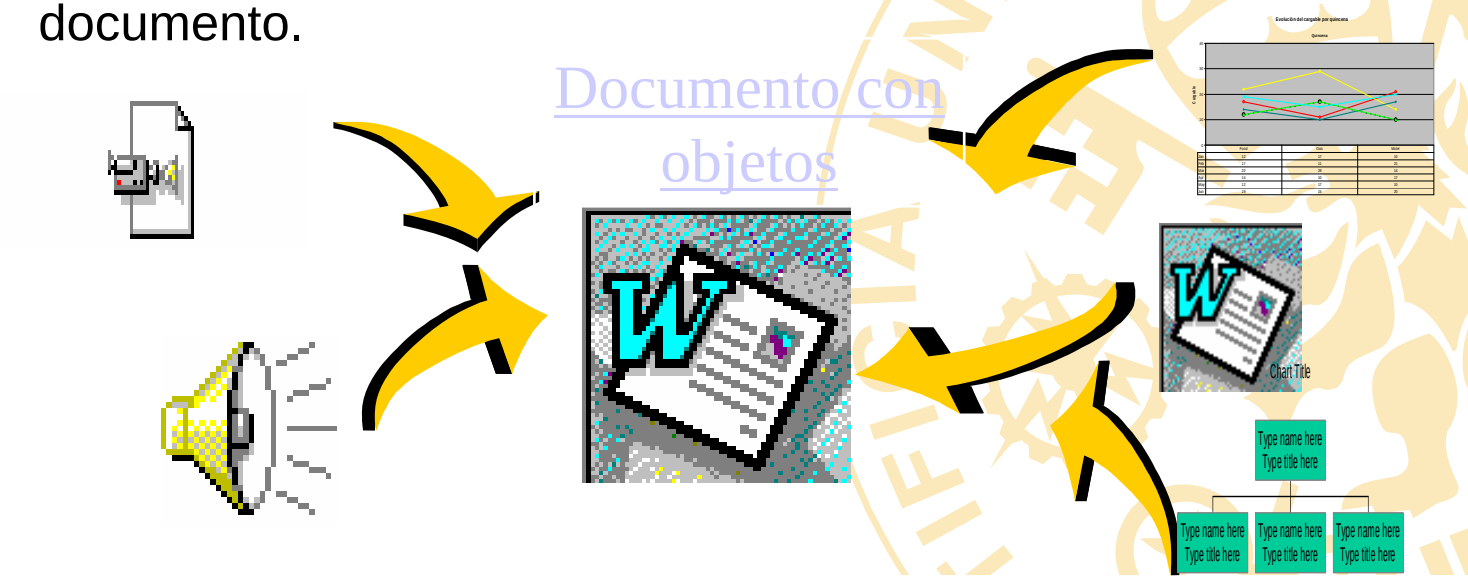
LOS VIRUS DE MACRO INFECTAN DOCUMENTOS

- **Se difunden más rápidamente**, por cada programa bajado de Internet, se bajan 245 documentos.
- Aparecen como consecuencia de malos diseños de los lenguajes de macros
- Hoy en día no son muy populares



Virus de macro (2)

- Los documentos (datos) son cada vez mas complejos.
- Dentro de un documento se pueden insertar objetos (imágenes, animaciones, música, otros documentos, etc.) y una clase de objetos que se pueden almacenar son programas escritos en VisualBasic (VBA).
- OLE es una metodología desarrollada por Microsoft para poder manejar objetos y dentro de OLE existe el formato de archivo “Compound File” para almacenar objetos dentro de un documento.



Virus de macro (3)

Características

- Un virus de macro puede hacer el mismo daño que un virus de programa. En el peor de los casos, **puede transportar un virus de programa** y ser activado al abrir el documento.

- Un virus de macro es MULTIPLATAFORMA, es decir puede afectar a cualquier plataforma donde se pueda utilizar Word o Excel (W98, WNT, W2K, Macintosh,....)

Virus de macro (4)

Virus de MS-Word

- Dentro de un documento de Word, parte del documento contiene la definición de macros, que permiten automatizar tareas repetitivas, por ejemplo, aplicar un estilo a parte del documento.

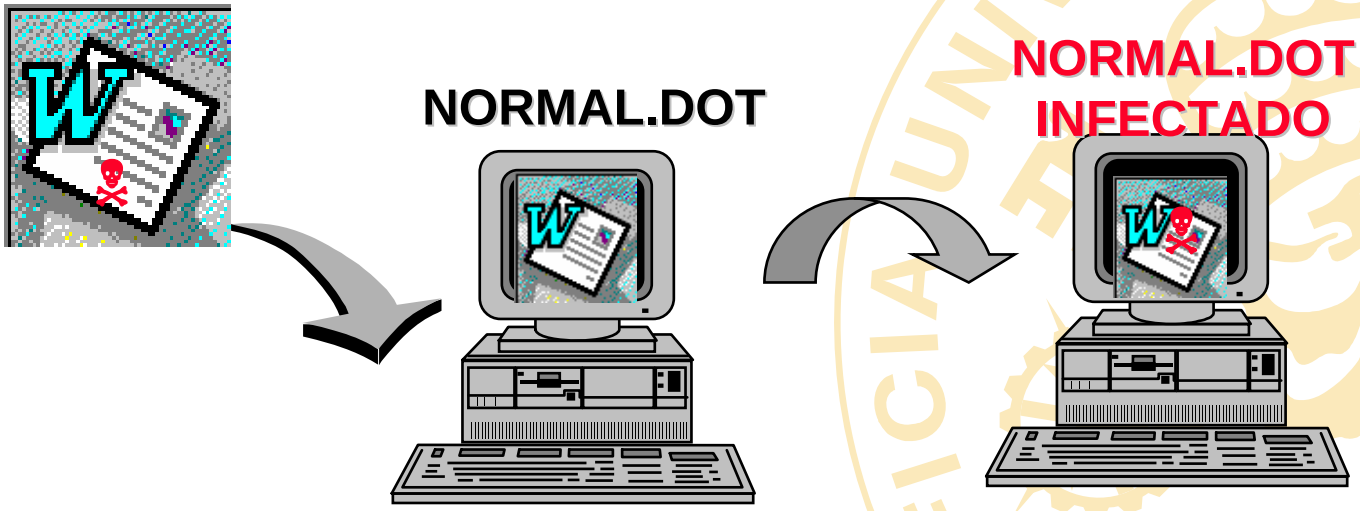
- Existen macros especiales que se ejecutan de forma automática: Las macros automáticas. Pueden ejecutarse al abrir un documento (AutoOpen), al cerrar un documento (AutoClose) y en otros casos (AutoExec, AutoSave, etc.)

- Los virus de macro utilizan macros automáticas para ser ejecutados cuando el documento es abierto.

Virus de macro (5)

Virus de MS-Word: **Infección inicial**

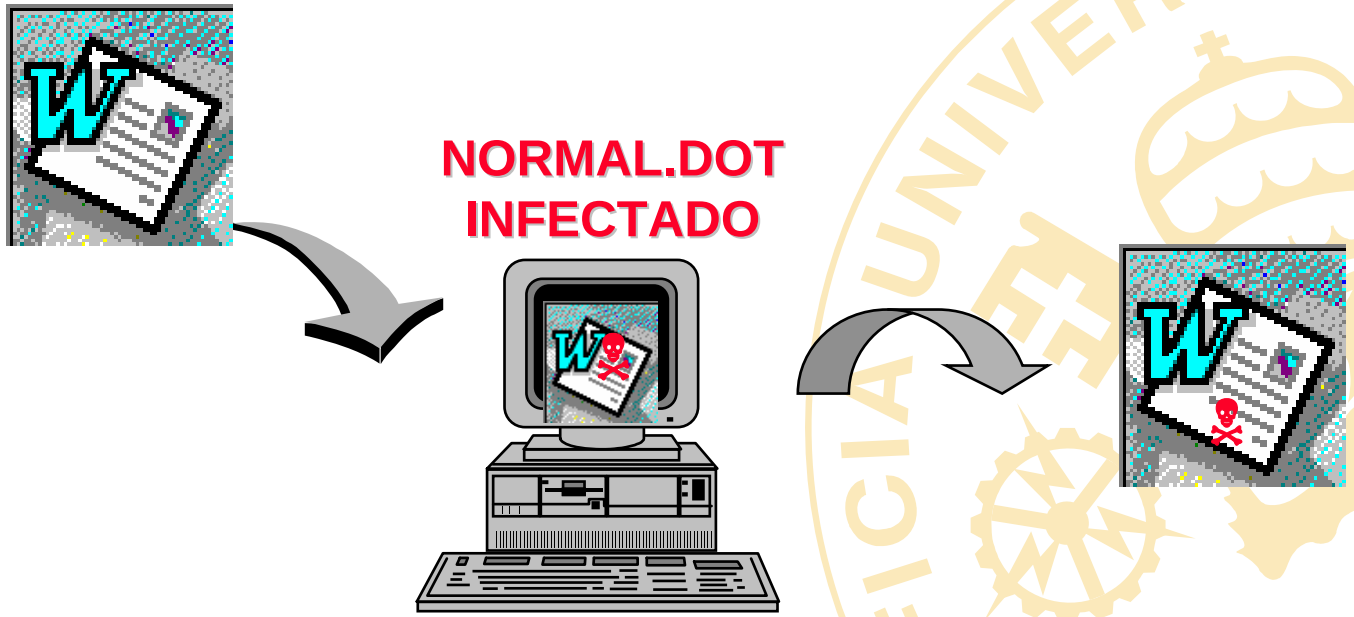
- Un virus de macro se ejecuta al abrir el documento (AutoOpen).
- Graba todas las macros en el NORMAL.DOT. Este archivo contiene las macros comunes a todos los documentos.
- Desde la plantilla NORMAL.DOT pasan las macros a cualquier documento que se abra.



Virus de macro (6)

Virus de MS-Word: **Propagación**

- Desde la plantilla NORMAL.DOT pasan las macros a cualquier documento que se abra.
- Al salvar el documento se guardará con el virus..

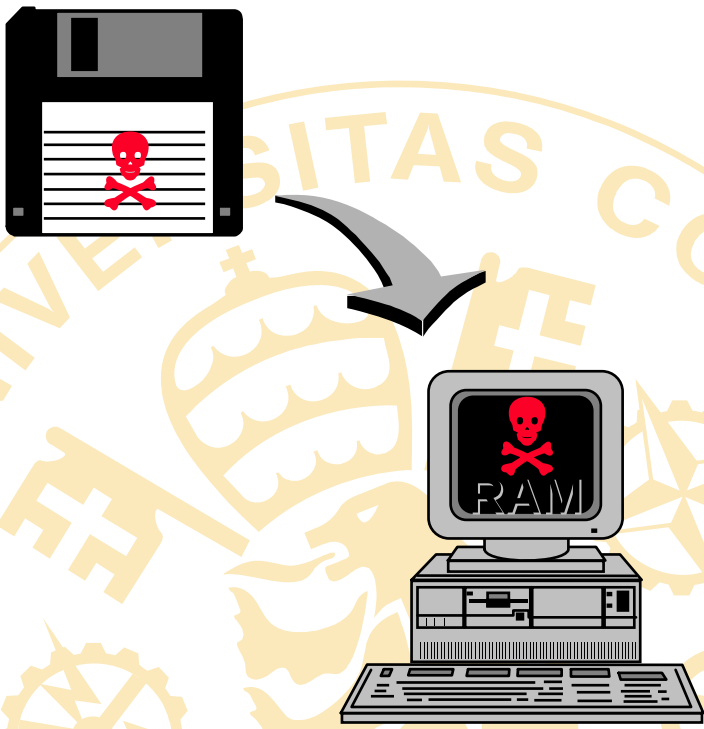


Virus de sector de arranque (1)

- Afectan a sectores reservados al sistema operativo
  - Sector de arranque de discos duros y disquetes
  - Tabla de partición de discos duros

- Los virus “puros” de sector utilizan el sector de arranque de los disquetes para propagarse.

- Existen virus de fichero ejecutable que también infectan sectores.



Virus de sector de arranque (2)

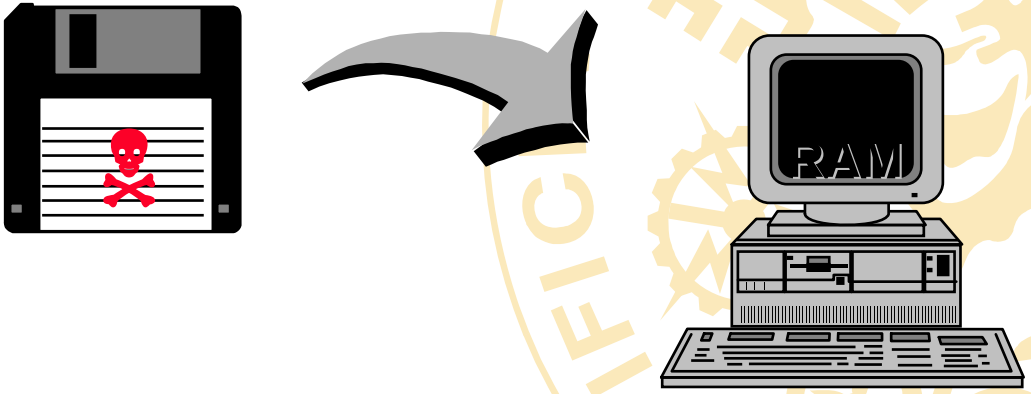
Características

- Suelen sustituir el sector que infectan por una versión propia pero conservan el sector sustituido para
  - Poder arrancar
  - Utilizarlo en técnicas de ocultamiento
- Es común que su tamaño sea 512 bytes o múltiplos de este tamaño
- Pueden extenderse a muchos diskettes antes de ser detectados, porque sólo se cargan al arrancar desde diskette
- Hoy en día son poco utilizados porque el proceso de propagación es demasiado lento para que sean efectivos

Virus de sector de arranque (3)

Infección inicial

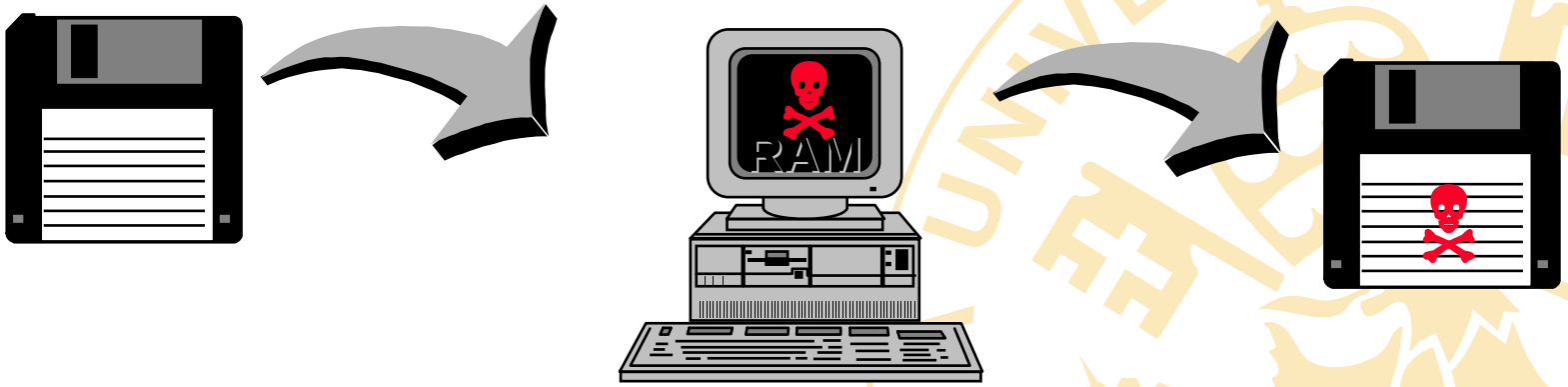
- Al encender un ordenador con un disquete infectado en la disquetera
  - Por el proceso de arranque de un PC el sector de arranque del disquete se carga y ejecuta en memoria RAM.
  - Ello permite al virus acceder a memoria RAM y ejecutarse
  - Infecta entonces el sector de arranque del disco duro



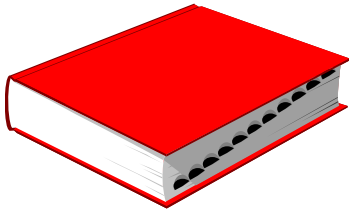
Virus de sector de arranque (4)

Propagación

- Al realizar alguna operación de E/S sobre un disquete
- Si el disquette está protegido contra escritura no se puede propagar



Virus de sector de arranque (5)



Resumen

- Afectan a sectores reservados al sistema operativo
  - Sector de arranque de discos duros y disquetes
  - Tabla de partición de discos duros
- Sólo se produce la infección al arrancar el ordenador con un disquete infectado (o mediante algunos virus de programa concretos)
- Utilizan el proceso de arranque de un PC para acceder a memoria
  - La mayoría de las BIOS actuales permiten definir la secuencia de arranque, para utilizar sólo el disco duro principal
  - La mayoría de las BIOS incorporan protección contra estos virus evitando acceder a los sectores de arranque y tablas de partición

Virus de sector de arranque (6)

Auto-arranque de CDs

- Es la forma moderna ya que los CDs han sustituido a los diskettes.
- Resulta incluso más peligroso porque se activan en cualquier momento (autorun) con sólo insertar el CD y sin necesidad de reiniciar el ordenador.
- En un experimento realizado por Training Camp (UK)
  - Se repartieron CDs en el metro.
  - El CD contenía un troyano que símplemente enviaba una confirmación de instalación.
  - Se recibieron señales de bancos, compañías de seguros, etc.

Virus de Internet (1)

- Cada vez se utilizan menos diskettes para transferir información y hay una clara tendencia a utilizar Internet.

- Existen varios mecanismos para transferir por la red programas ejecutables o archivos que contengan virus. La manera más probable de recibir un virus es por medio de alguno de estos mecanismos.

- La mayoría de los virus y worms que aparecen hoy en día están diseñados para propagarse por Internet de manera automática.

Virus de Internet (2)

Mecanismos de propagación

- e-Mail: Propagación masiva. Happy99, I-Worm exploreZip
- Carpetas compartidas
- News, FTP, servidores de aplicaciones
- Chat: programa mIRC que soporta scripts
- Navegación Web: rutinas VBS ocultas en html, o rutinas JavaScript (mucha menor incidencia)
- Java: Se ejecutan en la máquina virtual, con acceso a recursos muy limitados
- Active X: Tienen total acceso al S.O. Windows. Se utilizan mecanismos de firma electrónica para asegurar un origen fiable.
- Agujeros de seguridad. Por ejemplo IIS y SQL Server

Virus de Internet (3)

Efectos que producen

- DoS: Denegación de servicio debido al incremento del tráfico de la red.
- Los efectos de cualquier virus
- Muchos troyanos abren una puerta en el sistema (back door)
- Ataques DoS coordinados contra un servidor concreto.

Virus de Internet (4)

Módulos que pueden incorporar

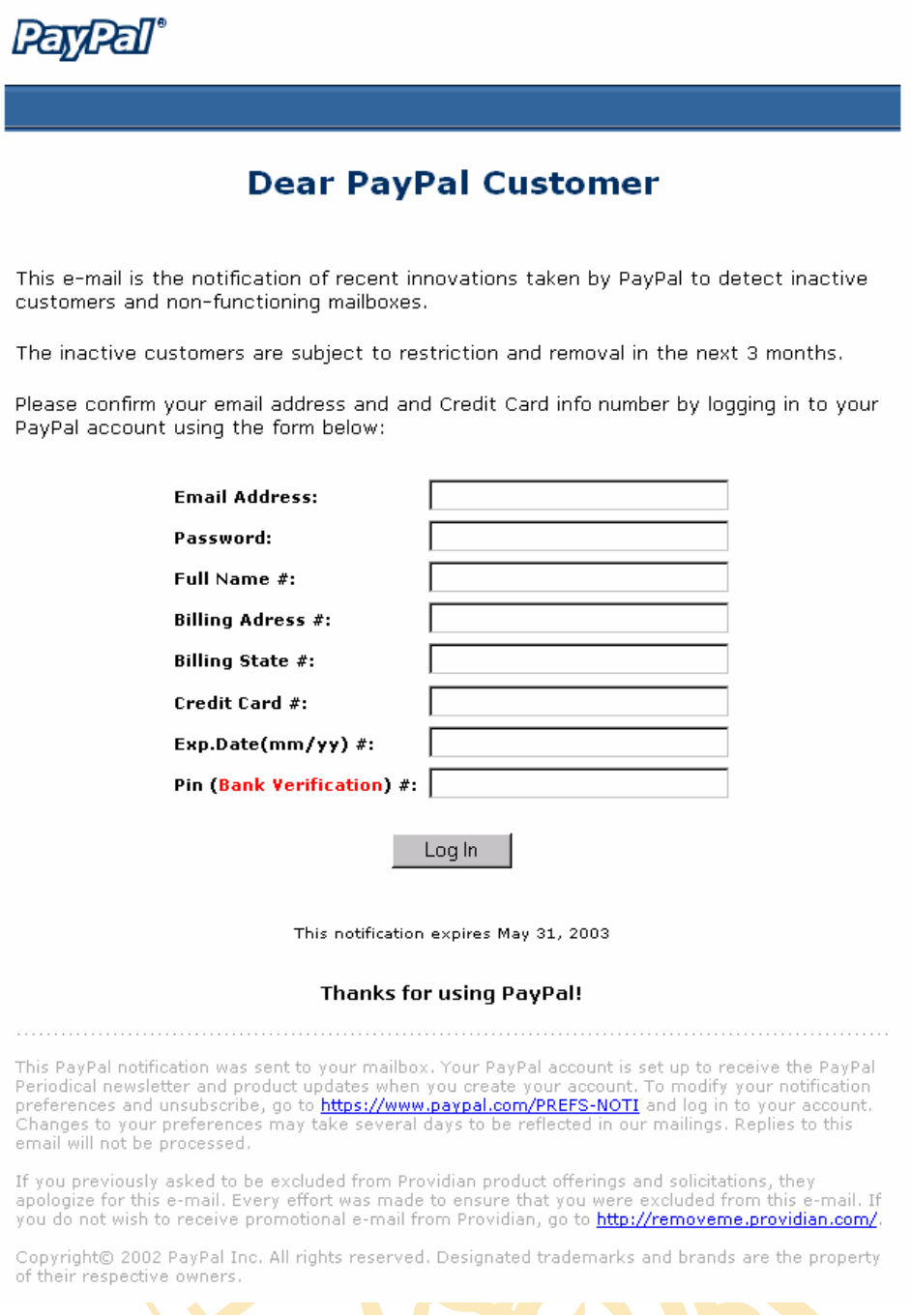
- Lectura de la agenda y de las carpetas de mensajes de correo
- Servidores SMTP propios
  - Se pueden reenviar sin depender de un cliente de correo particular
  - Fácilmente pueden falsear el remite del correo
- Módulos de propagación por carpetas compartidas
- Módulos de conexión por TCP/IP a puertos concretos
- Ocultación y anulación de antivirus
- Activación automática (antiguas vulnerabilidades de Outlook)

Técnica de phishing (1)

- **Mensajes engañosos** desarrollados obtener información confidencial
- Se basan en el correo spam y en la incultura informática de los usuarios
- El mayor peligro está en claves de acceso bancario y números de tarjetas de crédito.
- Ejemplos: PayPal (may 2003), Banco Popular (ene 2004), Banesto (ene 2004)

phishing (2)

Formulario del engaño PayPal



PayPal

Dear PayPal Customer

This e-mail is the notification of recent innovations taken by PayPal to detect inactive customers and non-functioning mailboxes.

The inactive customers are subject to restriction and removal in the next 3 months.

Please confirm your email address and and Credit Card info number by logging in to your PayPal account using the form below:

Email Address:
Password:
Full Name #:
Billing Adress #:
Billing State #:
Credit Card #:
Exp.Date(mm/yy) #:
Pin (Bank Verification) #:

Log In

This notification expires May 31, 2003

Thanks for using PayPal!

This PayPal notification was sent to your mailbox. Your PayPal account is set up to receive the PayPal Periodical newsletter and product updates when you create your account. To modify your notification preferences and unsubscribe, go to https://www.paypal.com/PREFS-NOTI and log in to your account. Changes to your preferences may take several days to be reflected in our mailings. Replies to this email will not be processed.

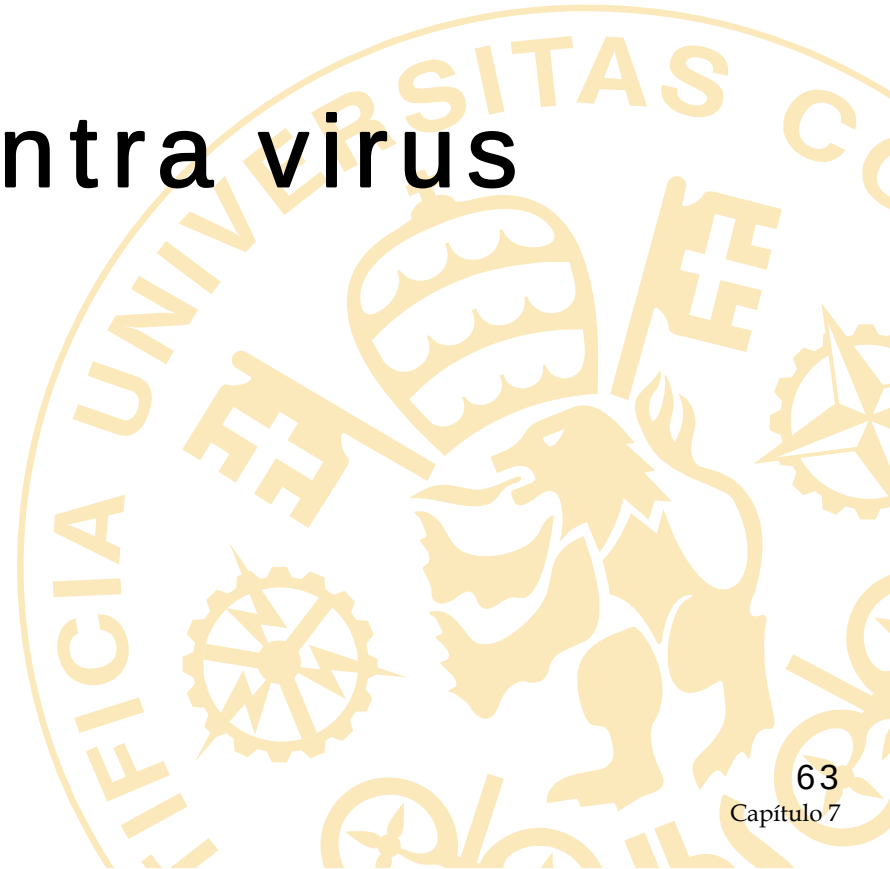
If you previously asked to be excluded from Providian product offerings and solicitations, they apologize for this e-mail. Every effort was made to ensure that you were excluded from this e-mail. If you do not wish to receive promotional e-mail from Providian, go to http://removeme.providian.com/.

Referencias sobre phishing

- Federal Trade Commission, "How Not to Get Hooked by a 'Phishing' Scam", http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm

- Anti-Phishing Working Group, http://www.antiphishing.org/

Protección contra virus



Protección contra virus

- Consejos de buena conducta
- Métodos preventivos/correctivos: antivirus
- Productos comerciales
- Pruebas de detección
- Protección perimetral

Consejos de buena conducta

- Imponer medidas y políticas de seguridad corporativas. Campañas de información a los usuarios
- No ejecutar programas que lleguen en correo electrónico (aunque sean de personas conocidas)
- Instalar los parches de seguridad de los programas.
- Mantener siempre activo antivirus en servidores y estaciones
- Actualización constante del antivirus
- Utilizar siempre software fiable
- Controlar discos de procedencia ajena
- No utilizar el disco duro como único lugar de almacenamiento
- Cuidado con los portátiles
- Analizar todo el ordenador periódicamente
- Escanear todo el tráfico de entrada/salida

Métodos preventivos/correctivos: antivirus (1)

- Los paquetes antivirus utilizan diferentes técnicas de detección
  - **Búsqueda de cadenas** que identifican virus
  - Búsqueda **deductiva**, determinan si un fichero está infectado o no, observando varios parámetros
  - Búsqueda **heurística**, desensamblando el virus y buscando secuencias de instrucciones de virus (nivel de precisión aceptable para virus conocidos y desconocidos)
  - Otras técnicas: Investigación. Pone a prueba el virus residente y todavía no detectados

Métodos preventivos/correctivos: antivirus (2)

- Ventajas de las técnicas avanzadas de detección
  - Permite detectar virus que implementa técnicas de ocultación
  - Permite detectar virus nuevos sin necesidad de actualización
  - Son eficaces para detectar variantes de virus existentes*

* Por ejemplo: El antivirus NOD32 detectó la variante de "Win32/Bagle.B" mediante técnicas heurísticas antes de que apareciese la actualización el 17/02/2004 14:54:52 (UTC+1)

Productos comerciales (1)

- Módulos que incorporan los antivirus
  - Detección y limpieza de archivos
  - Detección y bloque de tráfico de red
    - Filtros específicos POP, IMAP, SMTP, SMB, HTTP
    - Filtros tipo firewall (entrada y salida)
  - Filtro anti-spam → importante para evitar phishing
  - Detección de programas de hackers

Productos comerciales (2)

Fabricantes de Antivirus

- Network Associates (**McAfee**) – VirusScan (http://www.mcafee.com)
- **TrendMicro** – OfficeScan (http://www.trendmicro.com)
- **Symantec** – Norton Antivirus (http://www.symantec.com)
- **Panda** Software – Panda Antivirus (http://www.pandasoftware.com)
- **NOD32** (http://www.nod32.com)
- **Kaspersky** (http://www.kaspersky.com)
- **Sophos** (http://www.sophos.com)

Utilizar productos certificados por ICSA (http://www.icsalabs.net)

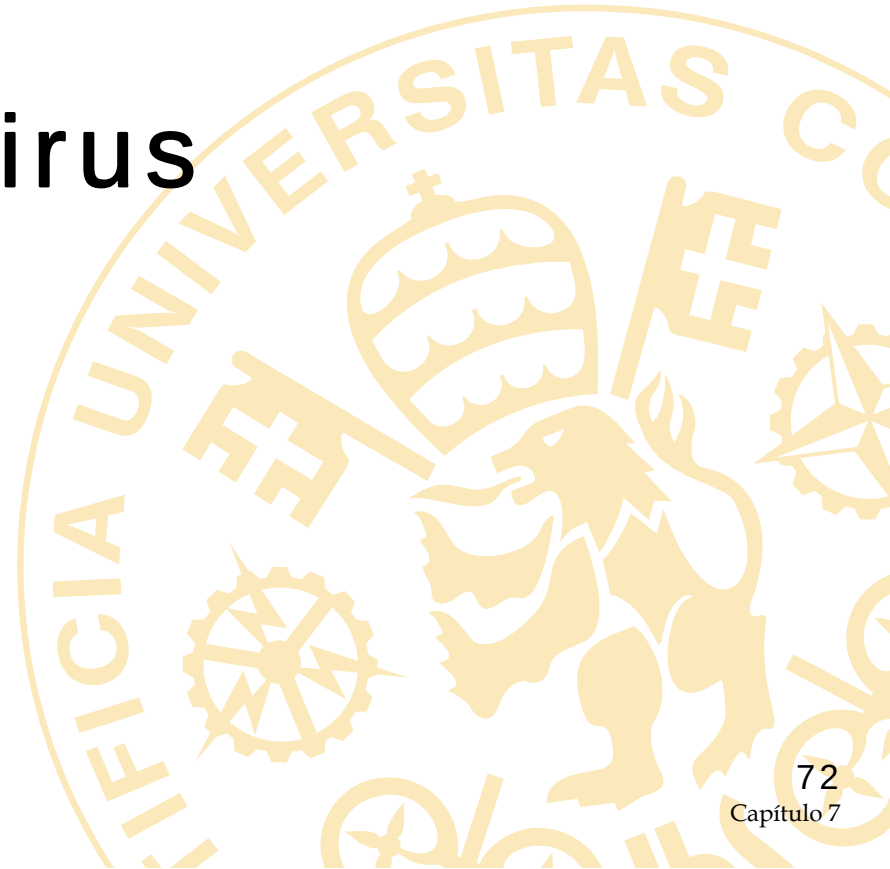
Pruebas de detección

- Es importante verificar periódicamente que los antivirus de los usuarios están actualizados.
  - Todos los antivirus modernos incluyen mecanismos de actualización automática
  - Algunos antivirus permiten verificar el estado en remoto; nos vale para comprobar que la actualización automática está bien configurada.
- EICAR es un virus de pruebas (no dañino) que es reconocido por cualquier antivirus.
  - Es el único virus que se puede utilizar para realizar pruebas
  - Está disponible en http://www.eicar.org/

Protección perimetral

- Supone una barrera entre Internet y la red local
  - Firewall para evitar ataque contra puertos concretos del PC (tipo winnuke)
  - Antivirus del servidor de correo (algunos revisan los mensajes almacenados)
  - Filtrado tipo anti-spam: basados en el análisis del asunto y contenido de los mensajes
- Pueden causar una falsa sensación de seguridad, por ejemplo los portátiles se saltan estos filtros.

Ejemplos de virus



Ejemplos de virus (1/9)

- Anna Kournikova. Fichero disimulado con .JPG Reenvio por email
- Love Letter: Gusano que se extendió muy rápido bloqueando muchos servidores de correo
- Melissa: Macro de MS-Word con gusano
- SirCam: “Te mando este archivo para que me des tu punto de vista” Con doble extensión
- Ramen: Para Linux
- CodeRed: Gusato para IIS (Internet Information Services)

Ejemplos de virus (2/9)

- Worm_Klez: (17/abr/2002, muchas variantes)
  - Explota vulnerabilidades de **Outlook**
  - Reenvío por correo electrónico con remites falsos. Obtiene direcciones de las carpetas de correos.
  - Utiliza subjects variables. Difícil de interceptar en servidores.
  - Se propaga también por archivos ejecutables conservando el tamaño original del ejecutable (algoritmos de compresión).
  - Intenta parar los antivirus.

Ejemplos de virus (3/9)

- Sobig (10/ene/2003)
  - Programa ejecutable
  - Reenvío por correo electrónico con servidor **SMTP propio**. Obtiene direcciones de las carpetas de correos, bases de datos etc.
  - Se propaga también por la red local copiándose a **carpetas compartidas**

Ejemplos de virus (4/9)

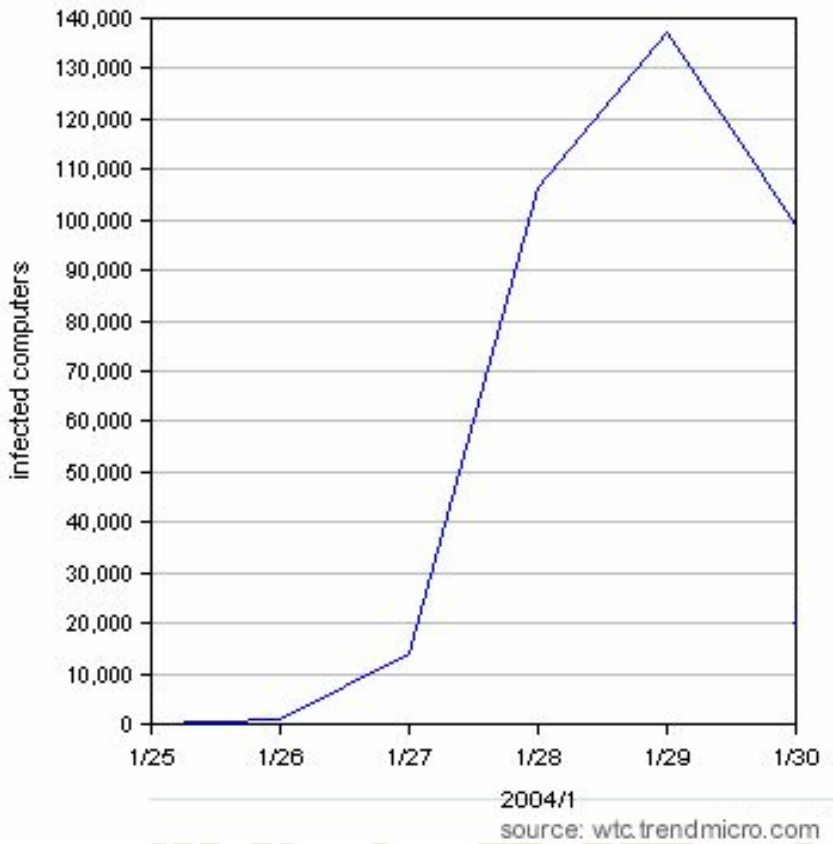
- Yaha (24/dic/2002)
  - Programa ejecutable
  - Reenvío por correo electrónico con servidor **SMTP propio**. Obtiene direcciones de muchas fuentes:
    - Windows Address Book (WAB)
    - Yahoo Messenger
    - MSN and .NET messenger Services
    - archivos con extensión HT
  - Utiliza remites, subjects, textos de correo y nombre de attachment (.exe ó .scr) aleatorios
  - Intenta parar los antivirus
  - Tiene varias fechas de activación

Ejemplos de virus (5/9)

- SQL Slammer (25/ene/2003, 5:30 AM UTC)
  - Internet worm contra Microsoft SQL server
  - En pocas horas 700.000 servidores web afectados
    - American Express network
    - 13000 cajeros automáticos de Bank of America
    - Tráfico telefónico en Finlandia
  - Coste estimado a la economía mundial: 1.000 millones de dólares. (Costes de productividad y oportunidad de negocio).
  - El parche estaba disponible desde julio/2002

Ejemplos de virus (6/9)

- 26/ene/2004, MyDoom worm
  - Internet worm contra sistemas Microsoft Windows
  - Correo electrónico basado en ingeniería social
    - Mensajes localizados en 142 países
    - Hasta uno de cada 3 mensajes tiene el virus (CNN)
    - > 400.000 ordenadores afectados
  - Ataques DoS programados:
    - 1/Feb/2004: www.sco.com
    - 3/feb/2004: www.microsoft.com

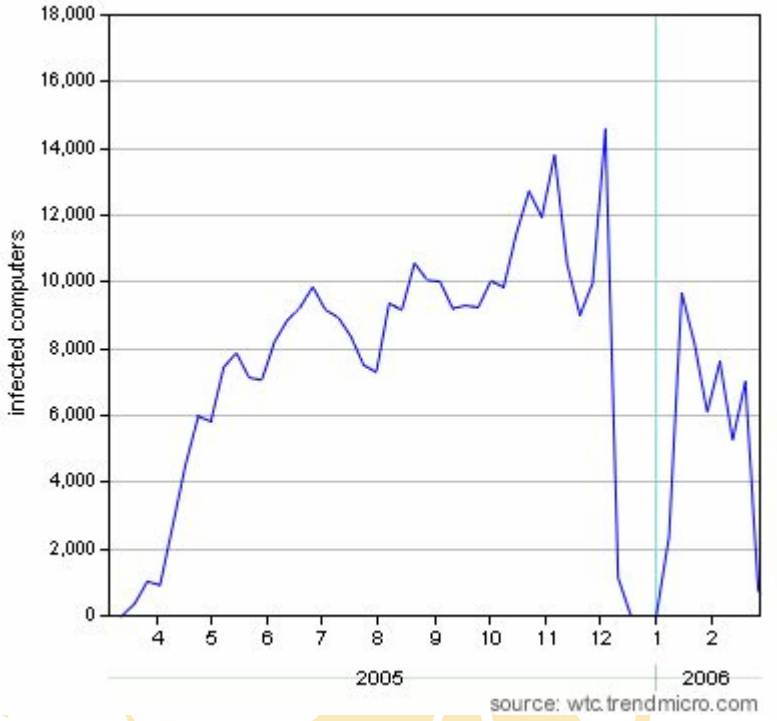


Ejemplos de virus (7/9)

Expansión lenta

- 24/mar/2005, SPYW_DASHBAR
  - Entra por Internet Explorer sin acción del usuario.
  - Instala un toolbar de búsqueda

  - Casi 400.000 ordenadores infectados



Ejemplos de virus (8/9)

Virus en la lista de alerta del Ministerio CyT

- 31/ene/2004, worm Sober.C
  - Fallo de configuración de la lista de correo de alertas del Centro de Alerta Temprana Antivirus.
  - Centro dependiente del Ministerio de Ciencia yTecnología a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.
  - Están reforzando la seguridad e incluirán firma electrónica en los mensajes.

Ejemplos de virus (9/9)

Sumitomo Mitsui Bank

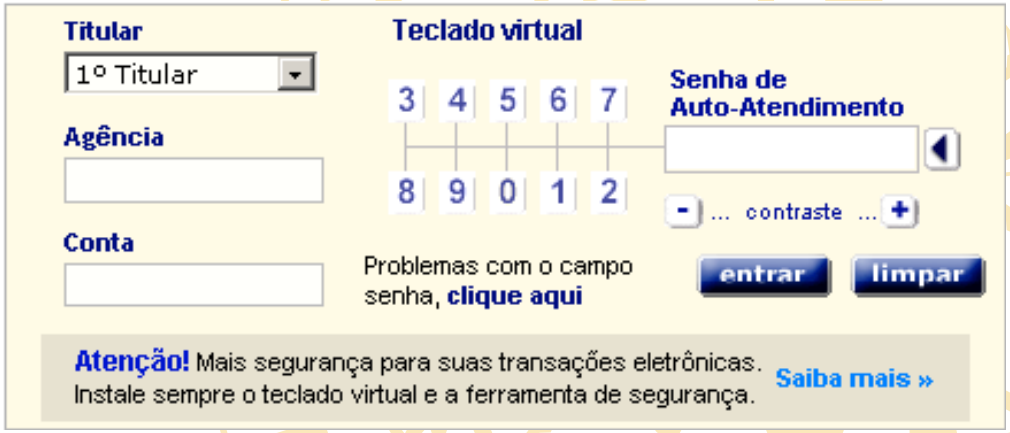
- 2005, programa keylogger
  - Se detectan transferencias sospechas
  - Intento de robo de $423.000.000
  - Se descubre un programa keylogger instalado en el ordenador de uno de los empleados del banco.

Ejemplos de virus (10/10)

videologgers (de keyloggers)

- 2006, troyano que captura video
  - Es una evolución de los keyloggers
  - Capturan la pantalla del ordenador en la zona del ratón (para ocupar menos espacio)
  - Evitan los teclados virtuales.

Ejemplo del Banco do Brasil



http://www.hispasec.com/laboratorio/troyano_video.htm

Resumen

Consejos Prácticos sobre e-mail

- Utilizar los protocolos seguros para descargar el correo: POPs, IMAPs. (Esto evita que nos roben el login y password)
- Desconfiar del remite de los correos
- Desconfiar de los correos que piden ser reenviados, y de los que contienen archivos adjuntos (ejemplo: "me, nude")
- Desconfiar de los avisos de virus
- No publicar la dirección de correo electrónico en web
- No enviar mensajes con copia a mucha gente, por ejemplo por cambio de dirección de correo (esto propaga las direcciones de correo y todos quedan expuestos a los virus)

Consejos Prácticos

- **Advertencias de tipo general**
  - Hacer backup regularmente
  - Bajar archivos de sitios fiables y verificarlos con antivirus o en www.virustotal.com
  - Bajar plug-ins o Extensions sólo de las fuentes originales
  - Desconfiar de archivos en CDs, Flash drives, diskettes
  - Utilizar protocolos seguros siempre que se escriban claves
  - Nunca dar ninguna clave a un banco (ni por teléfono, ni por correo, ni por web).
  - Manejar más de una clave.
    Ej. No utilizar la misma clave para el móvil que para la tarjeta de crédito.
  - Cuidado con los ordenadores prestados o cybercafés (stealthsurfer.biz).

Consejos Prácticos

Security is only as good as the weakest link. And most often, the weakest link is the human one.

Robert Lemos (SecurityFocus). PC Magazine 25(7), April 2006