Ética y Seguridad en la red II

Fernando Tricas García

ftricas@unizar.es

Dpto. de Informática e Ingeniería de Sistemas del Centro Politécnico Superior

Universidad de Zaragoza, España

http://www.cps.unizar.es/~ftricas/

Principios de Investigación en Medicina y Cirugía. Internet.

Burgos – 30 de enero de 2004

Los contenidos

- Contenidos indeseables
- Virus, troyanos y otros animalitos
- Compartir información

Contenidos indeseables

- Lo que no queremos ver
- En la red hay de todo (también cosas buenas. . . muchas)
- Educación
- Igual que en la calle (?)
- Hay filtros ...

Virus, troyanos, programas maliciosos

- Cualquier programa ‘extraño’ que ejecutemos es potencialmente peligroso.
- Incluso algunos aparentemente útiles
- No sabemos lo que puede hacer un programa de origen desconocido
- Lo mejor:
  - De alguna empresa ‘reconocida’
  - Que esté disponible el código fuente

¿Qué es?

Un virus es un programa de ordenador que puede infectar otros programas modificándolos para incluir una copia de sí mismo
Fred B. Cohen, en 1994 en su tesis doctoral.
Sólamente destructivos, molestos, ...

¿Qué es?

Un gusano es un programa que se reproduce, como los virus, pero que no necesita de otros programas para retransmitirse.

¿Qué es?

Un troyano es un programa malicioso que se oculta en el interior de un programa de apariencia inocente. Cuando este último es ejecutado el Troyano realiza la acción o se oculta en la máquina del incauto que lo ha ejecutado.
Cuidado!
Los troyanos fueron los atacados!

Hay más

- Pero hay más. . .
  - Espías (‘spyware’)
  - Servicios ocultos

¿Y los re-marcadores? (‘dialers’)

¿Cómo nos llegan?

- Programas normales infectados.
- Programas que producen efectos graciosos (felicitaciones, bromas, ...).
- Falsos antivirus
- Utilidades con truco

¿Cómo nos llegan? (II)

- Ficheros de contenidos para aplicaciones ofimáticas con capacidades programables.
  - .doc, .xls, .rtf falsos ...
  - Ficheros renombrados, enlaces falsos
  - Dobles extensiones

    LEEME.TXT.doc $\longrightarrow$ LEEME.TXT
- Aplicaciones de visualización de datos con capacidades programables.
  - javascript, VBS, ...
  - También pdf, Flash (.swf), ...

¿Cómo nos llegan? (III)

- Redes de intercambio de ficheros
- IRC
- Mensajería instantánea

Caso reciente: Mydoom

También conocido como Novarg, Shimgapi, Shimg, Mimail.R (lunes 26 de enero)

- Distribuido a través de adjuntos: .BAT, .CMD, .EXE, .PIF, .SCR y .ZIP
- El icono en windows simula ser un fichero de texto
- Dirección falsa
- Sigue....

Caso reciente: Mydoom

- Asunto variable (“Error”, “Status”, “Mail Transaction Failed”, “hello”, “hi”)
- Contenido textual variable ...
- Efecto
  - “Message” en el directorio temporal de Windows
  - “shimgapi.dll” y “taskmon.exe” en el directorio de sistema (system) de Windows (Uy!)

Caso reciente: Mydoom

- Abre “Message” (con caracteres al azar) en el bloc de notas.
  - Con este efecto el gusano intenta engañar al usuario.
- Busca direccciones de correo y se auto-envía
- Intenta reproducirse mediante Kazaa
  - winamp5, icq2004-final, activation_crack, strip-girl-2.0bdcom_patches, rootkitXP, office_crack, nuke2004
  - Abre el puerto TCP 3127 (¿puerta trasera?)

Caso reciente (cifras y letras)

- Hasta 1000 mensajes/minuto, (1 de cada 12)
- Un computador infectado envía mucho correo, pero también lo recibe
- Podría ser un ataque contra SCO (?) Se parará el 12 de febrero
- SoBig (agosto 03) causó millones en pérdidas (1 de cada 17)
- Slammer (enero 2003) era más rápido (red de cajeros automáticos del Bank of America). Infectó el 90 % de los servidores vulnerables en 10 minutos.

Caso reciente (principio de enero)

De: Grupo Banco <service@bancopopular.es>

Asunto: Importante informacion sobre la cuenta de Grupo Banco

Texto del mensaje:

¡Querido y apreciado usuario de Grupo Banco!

...

Despues del periodo de verifi cacion, sera redireccionado a la pagina principa de Grupo Banco. Gracias.

https://www2.bancopopular.es/[sigue dirección completa]

Caso reciente (pero menos)

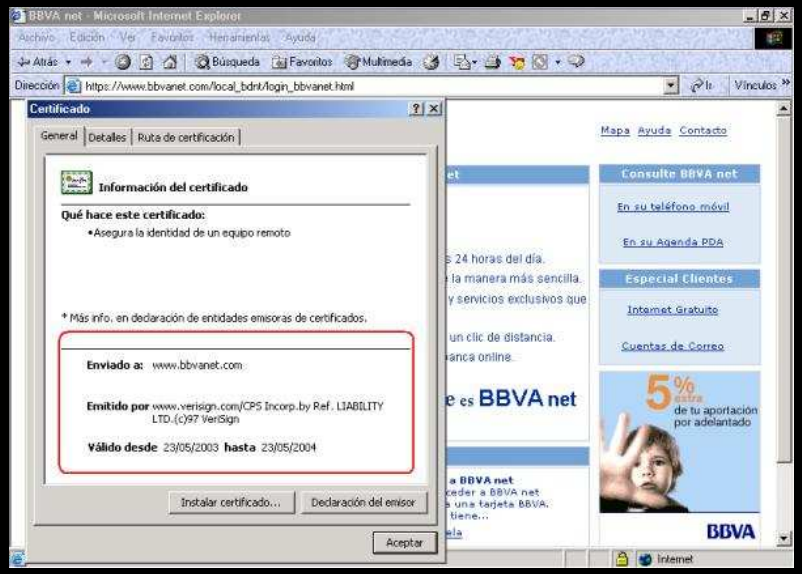
https://www2.bancopopular.es/

http://www.newmonc.com/!!!

¿Entonces?

- **https** sólo garantiza que la conexión es cifrada, no que sea ‘la buena’
- Comprobar que la dirección coincide con lo que esperamos (mejor, no pinchar en esa dirección, acceder como normalmente; si es imprescindible: copiar y pegar).
- Comprobar el certificado de autoridad
- También por correo electrónico
- En caso de duda ... teléfono, visita a la sucursal...

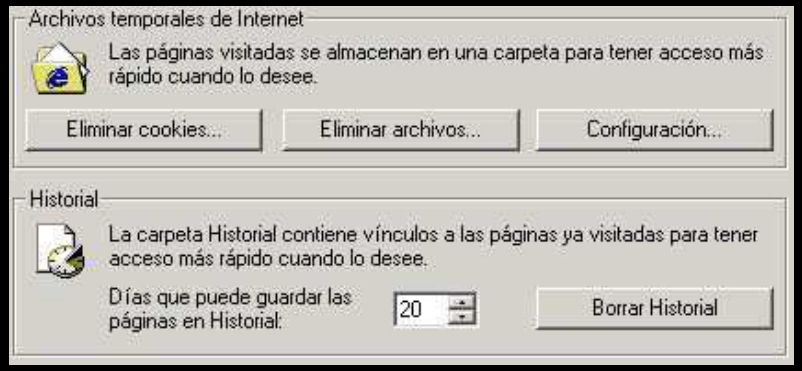
¿Dónde mirar?



El cerrojo

¿Algo más?

Borrar el historial ...



... sobre todo si el computador no es nuestro, o es compartido

Hace algo más . . .

MADRID.- Las felicitaciones de navidad y Año Nuevo que se reciben durante estos días por correo electrónico pueden ser un camuflaje perfecto para la propagación de virus por todo el mundo, según ha alertado hoy una empresa de seguridad informática. (El Mundo, 14-12-2001)
http://www.el-mundo.es/navegante/2001/12/14/seguridad/1008353205.html

---

Las detenciones, ocho de ellas en el Reino Unido, son el resultado de diez meses de investigación sobre las actividades de usuarios de portales de internet especializados en suministrar imágenes de pornografía infantil. (Estrella Digital, 28-11-2001)
http://www.estrelladigital.es/011128/articulos/espana/porno.htm

---

El plan del Gobierno de Estados Unidos para aumentar la seguridad interna llega también a la información, especialmente a la que cuelga en Internet. El objetivo de retirar provisionalmente información “comprometida"es evitar, entre otras cosas, que los datos que libremente se distribuyen en Internet puedan facilitar un nuevo atentado. (El País, 11-10-2001)
http://www.ciberpais.elpais.es/d/20011011/cibersoc/portada.htm

Algunas reglas de autoprotección

- Disponer de un antivirus (y utilizarlo, y actualizarlo).
- Suscribirse a las listas de avisos de seguridad (o tener a alguien que lo haga ...).
- Nunca ejecutar programas ni abrir ficheros del exterior (sin cuidado).
- Utilizar los perfiles de usuario.
- Ningún sitio serio (y los bancos lo son con estas cosas) le pedirá la clave nunca. De hecho, probablemente ni siquiera la conocen.

Algunas reglas de autoprotección

- Configurar adecuadamente los programas que interaccionan con el exterior (que no hagan nada, o casi nada, solos: atención a las previsualizaciones).
- ¿Realmente es necesario que me lo envíe así?
- Instalar y configurar adecuadamente un cortafuegos (*firewall*).

Algunas reglas de autoprotección

- Actualizar el sistema regularmente
  ... ¡cuidado! no fiarse de los avisos que llegan por correo, ir siempre a la página web del fabricante.
- Ni siquiera tienen nuestra dirección de correo, en caso de duda ..

Otras sugerencias

http://windowsupdate.microsoft.com
¡Una vez al mes! (segundo martes de cada mes)

Más autoprotección

- Estar preparados para lo peor (copias de seguridad).
- Comprobación del nivel de seguridad usado (¿pueden cambiarnoslo?)

Algunas reglas de autoprotección

- Los espías se usan para muchas cosas ...
  - Hábitos de navegación
  - Robo de claves
  - Robo de correo
  - ....

  Siempre: mucho cuidado con lo que instalamos.
  Hay programas para vigilarlos y eliminarlos.
  `http://www.seguridadenlared.org/es/spybot.php`

¿Y el spam?

- Correo no solicitado (de naturaleza comercial)
- Habitualmente, ofertas de dudosa condición
- Es muy barato para el que lo envía, y caro para los demás (sobre todo ISP’s)
- No siempre es inofensivo

¿Entonces?

- **Regla 1:** Hasta lo que parece inofensivo, puede ser peligroso.
- **Regla 2:** Cuanto menos automático, mejor.
- **Regla 2:** En caso de duda, preguntar.

Algunas aplicaciones

http://www.hispasec.com/software/checkdialer

http://www.seguridadenlared.org/es/checkdialer.php

http://www.seguridadenlared.org/

Más sugerencias

http://www.microsoft.com/technet/security/tools/mbsahome.asp

http://www.seguridadenlared.org/es/act-soft.php

Para NT, 2000 o XP.

Compartir archivos

- Compartir es bueno (la información quiere ser libre, sobre todo en la red)
  pero...
- Cuidado con los formatos (buscar el que menor daño pueda hacer)
- Cuidado con qué y de dónde viene
- Respetar la ley

Sobre las claves

- Que contengan mezcladas letras, números y otras cosas
  Z-89ñ.qe2
- Alrededors de 8 caracteres
- No compartirlas
  - Con los otros
  - Para varias cosas
- Cambiarlas de vez en cuando
- No sirve de nada una clave muy buena, si está al lado de la máquina en que se usa

Para saber más

- Criptonomicón

  `http://www.iec.csic.es/criptonomicon/`

- Campaña de seguridad de la Asociación de Internautas:

  `http://seguridad.internautas.org/`
  `http://www.seguridadenlared.org/`

- Hispasec

  `http://www.hispasec.com/`

- Muchas otras .... La seguridad está ‘de moda’.

Conclusiones

- La red fue diseñadad para dar fiabilidad y robustez, no seguridad.
- Mejor prudente y cuidadoso que tener las últimas herramientas informáticas.
- En algunos casos, la comodidad es enemiga de la seguridad.
- La seguridad es un proceso
- Seguridad como gestión del riesgo
- Disponemos de herramientas para garantizar nuestra privacidad, pero no sólo eso ...