Sobre virus y antivirus…

Ya hemos visto como desde Internet, podemos conseguir cualquier tipo de información, sobre (prácticamente) cualquier tema posible; también hablamos de los criterios a utilizar para determinar si esa información es, o no, fiable (uno de los riesgos inherentes al desarrollo de una plataforma en la que el principal control lo asumen los propios usuarios). En esta entrega intentaré exponer las pautas a seguir para evitar la actuación de uno de los peligros más frecuentes y dañinos que nos podemos encontrar en la red: los virus informáticos, también apuntaremos cómo luchar contra ellos (en caso de infección) y sobre todo, las reglas básicas de precaución para no correr más riesgos de los deseables .

La informática ha ido imponiendo su presencia en todos los ámbitos de la vida, lo que, si bien aporta notables ventajas tanto en el mundo de los negocios, como en el educativo, sanitario, militar…, también puede llevar aparejados inconvenientes y peligros, en algunos casos graves, que pueden resultar más o menos dañinos, en función del tipo de "ataque" al que nos veamos expuestos y el nivel de seguridad de nuestro equipo (desde bromas inocentes, hasta la pérdida total de la información archivada en el disco duro o la inutilización de equipos y las consiguientes pérdidas económicas que se deriven).

Un virus es una especie de programa informático; una secuencia de instrucciones codificadas en un lenguaje de programación específico (código malicioso), creada intencionadamente con un fin concreto (gastar bromas, recopilar y enviar información a terceras personas o empresas, robar información sensible o simplemente bloquear la red o causar daños en los equipos); que suelen introducirse en los equipos informáticos de manera involuntaria (sin el consentimiento del usuario).

Hay muchos tipos de virus y muchas formas de infección, así como también, múltiples maneras de combatir este problema; una de las maneras más efectivas es concienciar a los usuarios del problema y que éstos eviten acciones que pueden resultar inseguras; además de complementarlo con la instalación de programas y plataformas antivirus (programas que detectan y eliminan o bloquean la actividad de estos virus o códigos maliciosos). Pero vayamos por partes.

Aunque no se conoce a ciencia cierta, se cree que los primeros virus fueron creados en los años 60, como una especie de juego entre programadores y que poco a poco fueron sofisticándose (en 1987 una firma pakistaní, introdujo una secuencia en disquetes, que al ejecutarse inutilizaba el sector de arranque de los equipos en los que se introducían dichos disquetes, como venganza y escarmiento a los usuarios que los utilizaban con copias ilegales). El desarrollo de los virus, podría decirse que ha ido parejo al de la informática, aunque inicialmente la información sobre este tipo de problemas, no se divulgaba (las empresas no querían arriesgarse a perder la confianza de los clientes y los científicos y militares, evitaban hacer pública esta vulnerabilidad en un sistema que había costado millones de dólares), pero estábamos ante un problema imparable; cada vez aparecieron más, sucediéndose programas que se autoreplicaban y reenviaban por correo electrónico a otros equipos, haciendo que se colapsaran éstos y la propia red, hasta incluso llegar a bloquearla completamente. De esta manera se comprende como la generalización del uso del correo electrónico facilitó enormemente la difusión de los virus, pero hay otros sistemas de difusión (algunos muy difíciles de detectar por el usuario medio), que ponen en riesgo a cualquier equipo conectado a Internet, pues existen determinados archivos denominados "controles activeX", que se cargan automáticamente a nuestros equipos, solo con "navegar" por algunas páginas Web. Hay que tener en cuenta que un virus puede "esconderse" en prácticamente cualquier lugar, por lo que debemos estar alerta.

Vamos a diferenciar entre dos tipos de programadores, a los que se suele responsabilizar de la creación de virus; por una parte estarían los Hacker, o expertos que se dedican a detectar fallos de seguridad y otros problemas del software (programas informáticos); algunos se especializan en virus, pero principalmente para poder combatirlos; por otra parte estarían los Cracker, que si bien tienen un perfil similar, suelen estar fuera de la ley (se aprovechan de fallos de seguridad de los sistemas, para entrar en ellos, acceder a información privada, realizar estafas u otros actos delictivos, o simplemente alcanzar notoriedad. Aunque se les suele identificar a todos con el término Hacker, serían realmente los Cracker los que desarrollan y difunden los virus y demás códigos maliciosos.

Luís Arantón Areosa.
Enfermero.
Supervisor de Calidad del Área Sanitaria de Ferrol. A Coruña.

Correspondencia:
luaranton@gmail.com

Tipos de virus

Según su naturaleza y las funciones que tienen programadas, se distinguen tres categorías principales de virus:

- **Virus Convencionales:** Son programas maliciosos con capacidad de reproducirse, que se ocultan generalmente en archivos ejecutables (los que tienen extensión ".exe") y que pretenden dañar a los equipos a los que logran acceder (corrompen o borran archivos, bloquean el uso de algunos programas o simplemente ejecutan mensajes en pantalla o bromas u otras acciones que pueden resultar molestas). Suelen ser fáciles de eliminar de los equipos.
- **Troyanos:** Son una especie de aplicación que esconden un código malicioso que se activa al instalar el programa principal (pueden recopilar información privada para terceros, borrar archivos o incluso abrir vías de acceso "traseras" que podrían permitir el acceso y control del equipo de manera remota). Precisan que el usuario instale el programa huésped.
- **Gusanos:** Son programas que camuflados en correos electrónicos, se ejecutan automáticamente, replicándose y reenviándose (sin previa intervención del usuario) a las direcciones de correo que aparezcan en la agenda. Son los más difíciles de eliminar.

Las acciones que pueden llevar a cabo estos virus, en sus múltiples modalidades, van desde la destrucción o inutilización de archivos vitales del disco duro, a la saturación del sistema, con el consiguiente consumo de recursos y ralentización de los equipos; pero quizás la acción más preocupante, sea su capacidad de propagación, puesto que pueden llevarla a cabo de manera oculta, hasta que sea demasiado tarde para actuar (causan daños irreparables en tu equipo y al mismo tiempo en el de otras personas a las que puedan reenviarse o que utilicen tus mismos recursos).

Existen otros programas igual de peligrosos, que, si bien **NO** son propiamente virus, se engloban genéricamente en la denominación de **Malware**, (sofware que se utiliza para violar la seguridad de los equipos); algunos de los más extendidos son:

- **Dialer:** Son programas (marcado telefónico), que pueden generar conexiones telefónicas no solicitadas (generalmente a través de tarifas especiales) y dar lugar a facturas abusivas. Actúan solo en conexiones a través de modem (no en ADSL).
- **Backdoor:** Es un programa que modifica la configuración del equipo informático, dejando abierta una puerta de entrada al ordenador, que un atacante puede utilizar para espiar datos personales, instalar o copiar otros archivos o para hacerse con el control remoto del equipo.
- **Hoax:** Más conocidos como "engaños". Se trata de avisos de fallos, catástrofes, o intentos de recaudar dinero para causas aparentemente nobles, que se propagan por correo electrónico; también pueden tener afán difamatorio contra entidades o personas concretas.
- **Exploit:** Programas que aprovechas fallos en la seguridad de los sistemas operativos (u otros programas), para enviar programas dañinos, datos corruptos o para espiar información privada.
- **DoS:** Envían miles de consultas (al mismo tiempo) a un servidor para sobrecargarlo y bloquearlo; toma su nombre del mensaje de respuesta "Denial of Service".
- **Keylogger:** En realidad es un grabador de pulsaciones en las teclas; registra todas las pulsaciones sobre las teclas, con el fin de averiguar claves de cuentas u otra información privada.
- **Spyware:** Programa que se oculta en otro y que se instala al mismo tiempo que éste, enviando datos, costumbres, aficiones o historiales de navegación, al fabricante o a terceras personas, pero sin consentimiento del usuario.
- **Adware:** Son programas que también se ocultan en otros y se instalan conjuntamente; su misión es mostrar publicidad.
- **Phishing:** Aunque no es un virus, se ha incluido aquí por su peligrosidad. Se trata del envío masivo de correos electrónicos simulando que son de entidades bancarias, (imitan y muy bien a los correos originales de los bancos, con el mismo logotipo, etc), que con la excusa de solucionar un problema en nuestra cuenta, intentan conseguir que les enviemos nuestras claves o que accedamos a una dirección web que nos proporcionan (se trata de una página falsa, pero si entras, aparentemente es la oficial de nuestro banco) para que introduzcamos allí las claves y dar solución así, al problema que nos habían planteado. Hay que tener en cuenta que las entidades bancarias NUNCA solicitan esta información y mucho menos por vía electrónica, así que ante la duda hay que ponerse en contacto con ella, pero nunca a través del acceso que nos mandan en este e-mail.

  Que hacer si ha sido victima de esta estafa: Actúe rápido, cambie las claves privadas por otras nuevas, notifique lo antes posible la incidencia a su entidad (no espere al día siguiente), llame de inmediato (las entidades bancarias actuaran al instante y evitará pérdidas económicas que pueden llegar a ser importantes) y sobre todo, denuncie el fraude a las Fuerzas de Seguridad (la Asociación de Internautas ponen a disposición de todos los internautas que quieran reportar información sobre "phishing", la siguiente dirección: phishing@internautas.org

En resumen, muchos peligros son los que acechan nuestra aventura internauta; aquí, al igual que en lo referente a la salud, podemos asegurar que una buena prevención siempre será más que rentable; la solución pasa por responder a la siguiente pregunta: ¿que aspectos hemos, de tener en cuenta, para poder navegar tranquilos y sin demasiados sobresaltos?... casi siempre, como en otros aspectos de la vida, debemos hacer que impere la lógica.

SUITES y PROGRAMAS ANTIVIRUS COMERCIALES más conocidos

EMPRESA	CARACTERÍSTICAS	DIRECCIÓN
Panda Internet Security 2008	Es una suite de seguridad. Incluye entre otras aplicaciones Antispyware y firewall.	www.pandasecurity.es
Norton Internet Security 2008	Suite de seguridad, que incluye Antispyware, firewall y otras aplicaciones avanzadas.	www.symantec.es
Kaspersky Internet Security 7	Suite comercial similar a las anteriores.	www.bitdefender.es
Bitdefender Interney Security 2008	Completa suite (antivirus, antispyware, firewall)	www.mcafee.com/es
McAfee Internet Security Suite 2008	Suite antivirus con diversas funcionalidades	www.mcafee.com/es

Tabla 1.

SOLUCIONES ANTIVIRUS GRATUITAS

EMPRESA	CARACTERÍSTICAS	DIRECCIÓN
AVG Antivirus Free edition	Antivirus completo: protección residente, exploración de correo electrónico y actualización periódica de los patrones (disponible en inglés).	http://free.grisoft.com
Avira Antivir Personal Edition	Incluye escudo residente, detección de virus de macro y asistente de actualización. Disponible en Inglés y en Alemán.	http://seguridad-profesional.com/
Clam AntiVirus	Se distribuye con licencia GNU GPL2 (gratuito, código abierto). Protección permanente.Instalación algo compleja.	http://w32.clamav.net/
Avast 4 Home Edition	Gratuito para usuarios domésticos sin animo de lucro. En español.	http://www.avast.com/esp/download-avast-home.html
Spybot-S&D	Aplicación gratuita que analiza su PC en busca de software espía, publicitario, modificadores de navegador (hijackers) y otras aplicaciones de software malicioso.	http://www.safer-networking.org/es/download/index.html
Zonealarm	Cortafuegos muy potente y configurable que permite bloquear los puertos susceptibles de ataque. Dispone de versión de pago y gratuita.	http://www.todoprogramas.com/programa/zonealarmfree

Tabla 2.

Medidas de protección y antivirus

Una medida lógica es disponer de un buen antivirus. Un antivirus es un programa informático cuyo propósito es combatir y erradicar estos códigos maliciosos (virus y demás malware), pero hemos de tener en cuenta que tampoco esta medida es en si misma una medida definitiva:

1. Los creadores de virus, van siempre un paso por delante; cuando las empresas antivirus detectan un nuevo código malicioso, intentan responder en el menor tiempo posible, pero a veces los efectos destructivos ya han tenido lugar. Esta es la causa de que la principal recomendación sea que el antivirus (sea cual sea), siempre debe estar actualizado (cuanto más frecuente sea la actualización, mayor será su efectividad). Actualmente existen en el mercado soluciones antivirus para todos los gustos; algunas muy complejas y otras más sencillas; unas a precios más o menos asequibles y otras incluso gratuitas, pero no por ello menos eficaces. En las tablas 1 y 2, se relacionan los sistemas principales y sus características. Analiza sus características y decídete por el que mejor te convenza (no debes fiarte solo de la publicidad de las empresas).
   Los programas antivirus, actúan escaneando cada archivo del equipo (consumen recursos y pueden ralentizar los equipos) y los compara con las bases de datos de virus conocidos (actúan tras el ataque). Pero cada vez más antivirus utilizan lo que se llama técnica heurística, que se refiere a la capacidad de detectar situaciones de riesgo (secuencias que pueden corresponderse con códigos maliciosos), bloqueando su actividad e informando a la empresa antivirus, para que analice la situación y establezca una solución específica, si se confirma que es un virus (esta característica puede ser un argumento importante, a la hora de decidirnos por uno u otro sistema).
2. Muchos de estos virus, necesitan de nuestra participación para poder instalarse y llevar a cabo su cometido, por lo que hay que tener

MEDIDAS ANTIVIRUS

1. Antivirus instalado y actualizado (comercial o gratuito).
2. Sistemas Antispyware y Firewall complementarios (o integrados en la suite).
3. Utilizar particiones en el disco duro para separar el sistema operativo (programas) de la información (archivos); generalmente los virus afectan al programa operativo (no perderíamos los datos guardados en caso de infección).
4. Realizar periódicamente una copia de seguridad del registro de Windows y de los datos sensibles de su ordenador.
5. Utilizar con precaución el correo electrónico: no descargar (y ejecutar) archivos de origen desconocido o de procedencia dudosa.
6. No abrir o ejecutar archivos con extensión ".exe" sin comprobar su seguridad.
7. Extremar precauciones al utilizar programas de intercambios de archivos.
8. No responder a requerimientos realizados a través de correo electrónico, si no podemos identificar inequívocamente al remitente.
9. Denunciar cualquier intento de estafa o intrusión (phishing@internautas.org, http://www.delitosinformaticos.com/ciberderechos/direcciones.shtml, delitos.tecnologicos@policia.es)
10. Desconfía de los correos electrónicos, que aún procediendo de remitentes conocidos, incorporan archivos o programas que no hemos solicitado.

Tabla 3.

Imagen 1.

en cuenta una serie de medidas básicas a llevar a cabo por el propio usuario. Por muy bueno y potente que sea un antivirus, cuanto mayor sea la exposición a los peligros, más riesgo tendremos de que se produzca la infección. En la tabla 3, se resumen las medidas a tener en cuenta, para que la protección sea más efectiva.

3. Sea cual sea el sistema o sistemas empleados, el nivel de protección dependerá de la minuciosidad con que hayamos configurado dichas aplicaciones y programas; incluso desde el propio navegador puede aumentase el nivel de seguridad y de privacidad en la navegación y dificultar la aparición de problemas (imagen 1); aprovecha los recursos propios que te dan los programas.

Como medidas de protección adicionales, es conveniente utilizar algún otro dispositivo, que funcionando en segundo plano, nos aporte un nivel de seguridad extra, como son los **firewall** (más conocidos como cortafuegos, evitan el acceso externo a nuestro equipo, tanto de aplicaciones como de intentos de secuestro y control del equipo) o los programas **antispyware** que se encargan de detectar y eliminar los programas espía que se intentan instalar junto a otras aplicaciones aparentemente inofensivas. Muchos antivirus comerciales ya incorporan estas funcionalidades en sus ofertas de "suites" informáticas; pero hemos de tener en cuenta que también existen soluciones gratuitas, de las que podemos beneficiarnos.

En las páginas Web de las principales empresas de software antivirus, o en la enciclopedia Wikipedia, se puede ampliar información sobre estos y otros peligros, así como de la manera de prevenirlos y en su caso, de solucionarlos.

Agradecería cualquier sugerencia sobre los contenidos que os gustaría se abordasen en esta sección Tenéis a vuestra disposición mi correo electrónico (luaranton@gmail.com).

Gracias por estar ahí.