

Riesgos y amenazas

En este primer capítulo veremos cuáles son los peligros de la informática actual para, más adelante, analizarlos a fondo. Los principales conceptos sobre la prevención de virus, spyware, adware y ataques de todo tipo serán introducidos en las siguientes páginas, como también un panorama de la actividad del mercado de la protección.

Los peligros de la informática actual	14
Los virus, la amenaza histórica	15
La moda: adware, spyware y malware	16
Estafas electrónicas	17
Políticas de navegación	19
Resumen	19
Actividades	20

LOS VIRUS, LA AMENAZA HISTÓRICA

Los virus fueron una de las primeras amenazas en el mundo de la informática. Un virus es, en líneas generales, un archivo o un bloque de código agregado a un archivo cuyo fin es, además de reproducirse, generar alguna actividad dañina. Virus famosísimos como el **Michelangelo**, el **512** o el **LoveLetter** han sido tapa de diarios varias veces y han generado pérdidas millonarias en empresas y particulares desprevenidos.

La necesidad de estar protegido contra virus de computadoras es general, nadie (ni empresas ni particulares) quiere poner sus datos en riesgo y tener problemas con su equipo. El paso del tiempo ha demostrado que, aunque nunca parece ser suficiente, el uso de sistemas de protección por hardware y software disminuye radicalmente la posibilidad de infección y contagio de estos programas maliciosos.

Muchos usuarios se preguntan muchas veces sobre el origen de los virus, sobre cómo llegaron estos códigos a infectar sus computadoras. El mito sobre el origen de los virus dice que en la época de los disquetes de 5¼, los vendedores de software legal empezaron a hacer circular copias con virus (en ese momento, estos códigos aún no tenían un nombre) para infectar el incipiente mercado pirata y hacer que los usuarios desestimen la posibilidad de emplear programas ilegales ante la existencia de software legal y seguro. Esta práctica, si bien es impensable en la actualidad a causa de los avanzados sistemas de protección anticopia, era posible gracias a una característica específica de los disquetes, que podían ser sobrescritos aun siendo originales, ya que no contenían ningún método de protección más que la exigencia de una clave o un número de serie.

Lo cierto es que, con el devenir histórico, este origen aparentemente anticopia y ligado al ambiente del software legal de los virus cambió por un perfil más claramente político. Hoy los virus están creados usualmente por programadores que quieren manifestarse contra actitudes monopólicas o capitalistas, así como por aquellos que están en desacuerdo con la utilización de ciertos productos. No por nada la mayoría

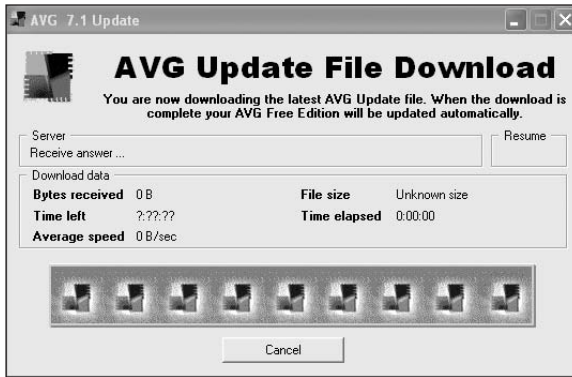


TODOS SOMOS IGUALES

Algunas publicidades dicen vender equipos seguros, aparentemente menos propensos a los ataques de las diferentes amenazas informáticas. Pero no hay que dejarse engañar: un equipo se vuelve más o menos vulnerable a los peligros de la informática según cómo está configurado y cuál es el uso que se le da. Nunca la configuración de hardware de un equipo determina su seguridad.

de los virus atacan el sistema operativo Microsoft Windows o sus aplicaciones, y son muy pocos los que tienen como objetivo destruir una instalación del sistema operativo Linux o de cualquier programa libre o de código abierto.

Actualmente, los virus no son la única amenaza informática, aunque sí siguen siendo la más peligrosa y, a la vez, la más temida. Hoy, los ataques a nuestra privacidad y la aparición de publicidad no deseada en ventanas del explorador de Internet merecen muchísima atención. Los programas que nos protegen de estos ataques, además, no son tan eficientes como los antivirus y ofrecen protección pasiva, lo que nos obliga a estar constantemente alertas.



En la imagen, vemos AVG Antivirus.

Figura 2. Un antivirus actualizado es esencial para trabajar con una computadora en Internet. Y el costo ya no es un problema: existen muchas opciones libres y gratuitas que funcionan perfectamente.

LA MODA: ADWARE, SPYWARE Y MALWARE

Los más grandes enemigos de los cibernautas y de sus computadoras son, en este momento, el adware y el spyware, molestos programas cuyo último fin es introducir publicidad no deseada en la máquina infectada. Aun cuando son muy poco dañinos, en la mayoría de los casos son las amenazas que más atentan contra el navegante.

Asociados con las prácticas publicitarias más ordinarias, los adware y spyware recorren Internet buscando equipos donde instalarse. Y lo más peligroso del asunto

PROTECCIÓN DE AVANZADA

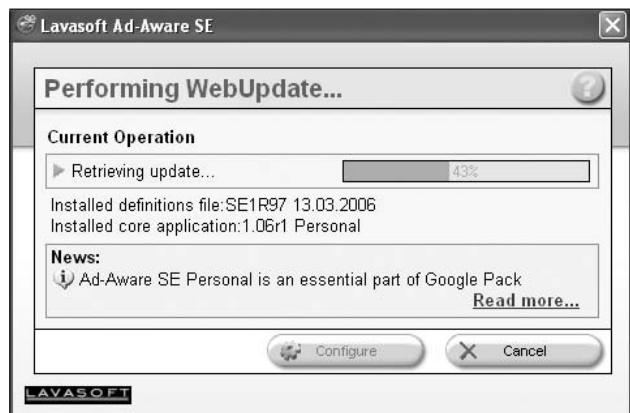
Los antiguos discos de 5 1/2 utilizaban como único método para proteger su sobrescritura una calcomanía que tapaba una muesca en el borde derecho del disquete. Los discos de 3 1/2 disponen de una traba plástica corrediza. El simple acceso a un disquete en una máquina infectada alcanzaba para introducir el código del virus. Estrategia impensable en los sistemas de escritura de CDs y DVDs.

es que una gran cantidad de programas instalan en la computadora del usuario más desprevenido estos elementos, que se encargarán luego de descargar más y más amenazas. Como ya dijimos, la causa de esto es la relación de la dupla adware/spyware con la publicidad: mucho software anunciado como gratuito se financia instalando en nuestras PCs spyware que supervisará nuestro comportamiento en la navegación y adware que descargará publicidad orientada, en teoría, a nuestros gustos. Así, las empresas pagarán a las compañías que incluyan adware y spyware en sus programas por cada descarga, que se convertirá en un nuevo punto de venta.

Si bien la inclusión de adware y spyware suele estar documentada en la licencia de los productos, es mínima la cantidad de usuarios que se detiene a leer este documento, presentado obligatoriamente en la instalación de todo software.

Cuando un spyware no está declarado en el Contrato de Licencia de Usuario Final (CLUF) o cuando un software es instalado con fines ilegales o de puro vandalismo informático, estamos hablando de malware. Si bien profundizaremos sobre el tema más adelante, el peligro de estos programas reside en su carácter fraudulento: la instalación de un malware en el equipo de cualquier usuario desprevenido podría convertirlo en un robot que reenvíe spam o ataque algún sitio (una **computadora zombie**, en la jerga), podría ser usado para cometer diversos fraudes informáticos, como robar y reenviar al programador los números de tarjetas de crédito o los datos de las cuentas de correo del usuario, etc.

Figura 3. Los removedores de adware y spyware también deben ser debidamente actualizados. De otro modo no se podrán eliminar todas las infecciones del equipo.



ESTAFAS ELECTRÓNICAS

Hemos repasado hasta ahora amenazas informáticas que, en última instancia, son programas o fracciones de programas que atacan equipos. Veamos ahora otras amenazas que atacan directamente al usuario pero no a través de programas, sino mediante el robo de datos, que el navegante ingresa engañado en algún tipo de formulario web.

Un ejemplo de esto es la técnica conocida como **phishing**, que consiste en enviar a los usuarios atacados e-mails que aparentan ser de compañías respetables y que piden la confirmación de algunos datos. Esta información ingresada por el usuario engañado es ilegalmente recopilada y se utiliza luego con propósitos fraudulentos. Del mismo modo actúan algunos sitios de Internet que son montados especialmente para cometer delitos contra los navegantes. Éstos exigen información para permitir el ingreso, y esa información luego será utilizada para atentar contra los navegantes.

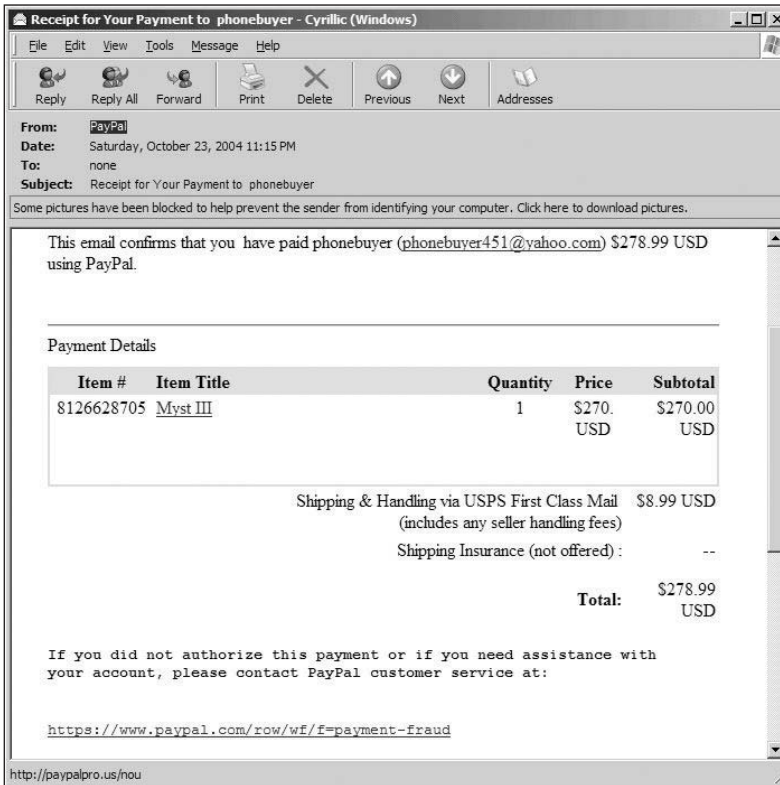


Figura 4. Un *phish* en Outlook Express: este e-mail pide confirmar nuestros datos de tarjeta de crédito para pagar una supuesta donación. Si ingresáramos nuestro número de tarjeta, estaríamos en problemas.

Aunque estas estafas son un tanto extremas y en promedio son pocos los sitios especialmente montados para defraudar usuarios, sí hay muchas variantes en sitios legales con las que hay que tener especial cuidado. Un claro ejemplo de esto son los recaudos que hay que tener a la hora de hacer circular nuestra dirección de e-mail: si brindamos nuestra dirección de correo oficial a cualquier sitio que nos la pida, no pasará mucho tiempo hasta que, misteriosamente, comiencen a llegar miles y miles de correos no deseados (spam) diariamente.

POLÍTICAS DE NAVEGACIÓN

En la actualidad, los usuarios de computadoras están expuestos a los peligros mencionados por el mero hecho de estar conectados a Internet. Por eso, es imprescindible que cada usuario sea consciente de las acciones que ejecuta al navegar, porque de su comportamiento depende el riesgo al que se expone en la navegación.

Es importantísimo entonces conocer plenamente lo que estamos haciendo y qué sitios estamos visitando durante nuestras vueltas por el ciberespacio. Y mucho más: no alcanza con tener cuidado al navegar, sino que hay que ser incluso más precavido a la hora de abrir e-mails y archivos adjuntos. La lista sigue, ya que también es un riesgo en potencia visitar y comprar en sitios de subastas electrónicas y de e-commerce si no se tienen recaudos.

Saber qué actitudes son seguras y cuáles inseguras en la red es fundamental. También, conocer los riesgos de todas y cada una de las actividades que hagamos en Internet: qué riesgos puede acarrear la visita a ciertas páginas, cuán seguro es jugar en red, qué hay de cierto en una ventana que se nos abre asegurándonos que somos los ganadores de un viaje al Caribe.

El objetivo fundamental de este libro es aprender una serie de políticas que debemos implementar a la hora de navegar para tener bien claro qué pasará al hacer cada cosa en Internet. Porque ése es el principal problema de la navegación: los usuarios no suelen tener del todo claro qué ocurrirá al hacer clic en cada vínculo.

RESUMEN

En este capítulo aprendimos que son muchas las formas de vandalismo informático que pueden atacar contra nuestra seguridad. Aunque en un comienzo el problema fueron los virus, el riesgo fue en aumento con la aparición de nuevas modalidades como el spyware, el adware y el moderno phishing. Lamentablemente, hoy en día no alcanza con protegerse de esas amenazas, sino que también tenemos que evaluar nuestras propias prácticas de navegación, ya que también ellas pueden poner en riesgo nuestra computadora y nuestros datos.



TEST DE AUTOEVALUACIÓN

- 1 ¿Sufrió alguna vez el ataque de un virus? Evalúe su experiencia.

- 2 Repase brevemente cuál es el origen de los virus.

- 3 ¿Por qué la tecnología de discos flexibles o disquetes propició la propagación de virus?

- 4 Diferencie virus de adware.

- 5 ¿Cuándo hablamos de adware y cuándo de malware?

- 6 Plantee la relación existente entre adware y spyware.

- 7 ¿Qué es un phish y cuál es su objetivo?

- 8 Exponga en qué casos sería seguro y en cuáles no comprar en sitios de subastas online.

- 9 ¿Cuáles son los más efectivos y famosos programas para combatir adware y spyware?

- 10 Explique cómo una red inalámbrica puede volverse insegura.

EJERCICIOS PRÁCTICOS

- ✓ Busque en Internet información sobre los virus Michelángelo, 512 y LoveLetter. Lea sobre los peligros de cada uno de ellos y la forma de defenderse.

- ✓ Haga un análisis crítico sobre sus prácticas de navegación. Tenga en cuenta su tendencia a navegar por sitios de empresas conocidas o no, su costumbre de lectura de advertencias y errores, etc.

- ✓ Ingrese en www.Download.com y lea las críticas y comentarios de los programas Lavasoft Ad-Aware SE y Spybot S&D.

- ✓ Haga una evaluación de lo leído en el punto anterior. Sobre la base de lo investigado, indique cuál elegiría para securizar su PC.

- ✓ Investigue en Internet sobre las amenazas del phishing y revise sus e-mails recibidos para ver si recibió algún correo de este tipo.
