EL FUTURO DE LOS ANTIVIRUS

"En los sistemas modernos hay demasiados tipos de archivos ejecutables, programas que pueden acceder a los componentes del computador. También es muy complicado que un sistema no tenga problemas, incluyendo agujeros de seguridad. Por todo ello, creo que los virus seguirán existiendo aunque el entorno contemple la seguridad basada en certificados digitales. .... Es posible desarrollar un entorno completamente protegido por la comprobación de firmas digitales, ¡pero los usuarios no lo usarán!, porque un entorno de este tipo no es lo suficientemente amigable... demasiadas limitaciones, demasiados avisos, demasiadas preguntas." Eugene Kaspersky

La inmensa mayoría de las infecciones víricas actualmente se deben a infecciones por gusanos (programas que se transmiten a través de las redes e Internet) y troyanos (los cuales suelen ejecutar acciones ocultas e indeseables) realizadas en su mayoría de las veces a través del correo electrónico. Estos virus se activan mediante la ejecución de adjuntos en el correo electrónico o simplemente mediante la lectura de correos recibidos con código malicioso dentro de HTML.

Existe la posibilidad que en el futuro aparezcan nuevos virus similares al Nimda o al Klez, los cuales podrán tomar ventaja de las vulnerabilidades existentes o de las que lleguen a presentarse. La educación y la conciencia basada en estrategias adecuadas de seguridad es la única forma de prevenir los posibles daños. Un posible colapso de la Internet (debido a una saturación del tráfico, a causa de los virus) no tiene tanto sustento a priori, pues sus límites antes que ser tecnológicos tienden a ser más bien culturales y ante una situación de esta naturaleza todavía se tienen elementos para prevenirla.

Hoy en día, dado lo sofisticado que son estos programas, uno solo de ellos tiene la característica que no le piden nada a sus antecesores, constituyendo de esta manera, la principal causa de los estragos producidos. El gusano Nimda (que llegó como troyano y destruye el sistema como un virus) y el Klez nos abren todo un abanico de posibilidades y sorpresas inesperadas que ponen a tambalear nuestros esquemas clásicos de protección.

Virus, Troyanos, y gusanos han existido desde los inicios de los sistemas operativos actuales y de Internet. La contienda “virus - antivirus” ya tiene sus dos décadas y nada nos indica que vaya a terminar. No se puede descartar, por ejemplo, que en un futuro cercano los virus atacarán teléfonos celulares programables y se propagarán cuando encuentren algún vínculo abierto entre dos aparatos. La principal vía de contagio, tal como hoy ocurre con las computadoras, será el correo electrónico, que ya está disponible en el mundo de la telefonía móvil.

Remarcando esto, los virus del futuro no sólo harán blanco en computadoras y servidores sino que serán diseñados para atacar teléfonos celulares inteligentes y asistentes digitales personales. Estos códigos maliciosos se prevé (esto es solamente un escenario o conjetura muy al estilo de Julio Verne) que incluso podrían llegar a grabar conversaciones y enviarlas vía correo electrónico a otros usuarios sin el consentimiento del dueño del aparato, suprimir o alterar estados financieros almacenados en los celulares, o incluso cambiar los números telefónicos contenidos en la memoria de estos artefactos y reemplazarlos con otros números de larga distancia, con el fin de generar cuentas y débitos de proporciones enormes.

Más aun, no es descabellado (no, al menos del todo) que las guerras del futuro cercano entre países desarrollados tendrán lugar entre dos redes informáticas, en las bolsas y mercados financieros interconectados, entre naves no tripuladas y satélites. De hecho, mientras el capitalismo prevalezca y esta situación nos alcance, las armas convencionales solamente se llegarían a utilizar con los países subdesarrollados.

Si miramos un poco al futuro y pensamos en la domótica (control de edificios, casas, etc, mediante hardware y software), vislumbramos ya la introducción de Internet en nuestra vida doméstica. De hecho, algunos operadores de televisión por satélite ya pregonan la disponibilidad de Internet a través de la televisión. De modo que tal vez dentro de poco, junto con nuestra televisión tengamos que comprar algún tipo de dispositivo antivirus. Y no pensemos sólo en la televisión, ya que otros electrodomésticos también serán alcanzados por los largos tentáculos de Internet.

El futuro nos augura mayor número de virus y más sofisticados, en lo que va del 2006 ya se ha sobrepasado la cifra que se tenía al cierre del año 2005. Algunas posibles tendencias pueden ser las siguientes:

1. Gran incremento en el número de virus, gusanos o backdoors. La frecuencia avasalladora con que van apareciendo nuevas variantes de malware (códigos maliciosos) nos predispone a mantener una política coherente y adecuada de actualizaciones. A la hora de escoger un software antivirus se ha de tener en cuenta la capacidad de actualización y la velocidad de respuesta de los laboratorios de las empresas, así como las capacidades heurísticas (detección de posibles virus nuevos) que tengan integradas estos productos.

2. Java y Actives. Ambos de estos componentes gozan presumiblemente de mecanismos de seguridad para evitar la difusión de virus pero tienen algunos agujeros (no son la panacea, pues de ser así, Windows XP sería una promesa verdaderamente mesiánica) . La seguridad de ActiveX se basa en que sólo puede ejecutarse código autenticado . Eso es mejor que nada pero aún deja mucho que desear, no se puede apostar a que autenticar sea una garantía absoluta o infalible.

3. Más conectividad. La demanda de mayor ancho de banda incrementa con cada vez más información en circulación. A mayor intercambio de información , mayor intercambio de todo tipo de programas o archivos incluyendo a los diversos gusanos que vayan surgiendo.

4. Lenguaje de macros más potente, universal y manejable. Los fabricantes de software incluyen cada vez lenguajes de macro más potentes y sencillos de utilizar pero como contrapartida, más vulnerables a los ataques o incorporación de códigos no necesariamente benévolos. Aparentemente los virus de macro ya no son los que dominan la escena, pero bien podrían irse

acompañando en el ciberespacio de gusanos cada vez más potentes (de hecho Melissa nos dio una adelanto de situaciones de este tipo) y de esta manera afianzar novedosamente su presencia.

5. Más virus destructivos. El código fuente del virus CIH (capaz de sobrescribir en determinadas circunstancias el BIOS y dejar la máquina absolutamente inoperante), los más diversos kits de creación de virus y otras tantas linduras están al alcance de todo mundo en Internet. Esta información alienta a otros programadores de virus a generar otros, e incluso a auténticos aficionados ("lamercillos" y crackers) a sentirse como niños en dulcería con el simple hecho de jugar con estas cosas.

Lo anterior nos lleva a pensar (sin mucho temor a equivocarnos) que el futuro de los antivirus está fundamentalmente en el desarrollo sólido de la heurística, y en la integración de éstos hacia una estructura más sólida de software que contemple a antivirus, cortafuegos, detectores de intrusos y autenticación como un solo producto.

REDESNA Informática S.L. espera que este artículo te haya sido útil !