boletín técnico®

imef ejecutivos de finanzas

NUM. 13 / 2004

COMITÉ TÉCNICO NACIONAL
DE TECNOLOGÍA DE INFORMACIÓN

Seguridad Antivirus

Ing. Arturo Fernández Maldonado

Introducción

Los virus informáticos han pasado a ser, para las empresas, una preocupación de alta prioridad, debido a que en ultimas fechas se han tenido ataques con mayor frecuencia.

Por lo tanto uno de los principales factores de riesgo para la operación y el funcionamiento de las empresas, son los "virus informáticos" ya que por su capacidad de dispersión y la combinación de múltiples tecnologías que logran rápidamente contaminar toda una red, ocasionando grandes pérdidas de información y pérdidas de tiempo y por consecuencia grandes pérdidas económicas.

En la actualidad se pueden observar un promedio de 500 virus nuevos al mes, cada vez más sofisticados, algunos de los cuales tienen como objetivo principal la "negación de servicios" en las redes informáticas de las compañías, aprovechando las vulnerabilidades de los sistemas operativos y sus sistemas de gestión.

Estos nuevos virus (o códigos maliciosos) cuentan intrínsecamente con procesos técnicamente complejos que les permiten ingresar a las redes corporativas a través de múltiples puntos de acceso en forma simultánea y desarrollar tiempos explosivos de propagación y modalidades avanzadas de infección.

Este nivel de "inteligencia" y complejidad técnica de las nuevas generaciones de virus, expone a las empresas a tener sistemas vulnerables o directamente infectados, a pesar de tener implementadas soluciones integrales de antivirus a lo largo de la organización.

Ante esta situación nos hacemos la pregunta:

¿Qué es un virus?

Un virus es un programa informático que tiene la facultad de replicarse y hacer copias funcionales de sí mismo una vez que ingresa a una computadora y distribuirse hacia otros archivos. Así como atacar a otros archivos y programas.

En la actualidad los virus informáticos han evolucionado de tal manera que ahora tienen la facultad de colapsar la redes informáticas mundiales en cuestión de minutos.

Pero conozcamos los diferentes tipos de virus que han existido y su desarrollo tecnológico.

Virus: Desarrollo y formas de ataque

Los virus informáticos han tenido una evolución muy rápida, con ataques muy precisos y tasas de infección que crecen

en forma exponencial a últimas fechas.

Etapas de Evolución de los Virus

1990-1992. Este periodo es dominado por los Virus de Arranque. Fueron los primeros virus que aparecieron y el ataque iba dirigido hacia áreas específicas de los discos flexibles (diskettes) y los discos internos de las computadoras de escritorio. La forma de notar que el virus estaba en la computadora era una lentitud sumamente notoria al encender el equipo y al trabajar con ella. Además de la pérdida de información. Algunos virus representativos fueron: NATAS, MichelAngelo.

1992-1995. En estos años aparecen los virus Macro. Los cuales son aquellos virus que se crean y ejecutan a partir de programas que permiten automatizar ciertas tareas que normalmente son rutinarias o se hacen a mano, como por ejemplo el caso de Microsoft Word que nos permite crear cartas. Si necesitamos enviar 500 cartas que parten de un mismo texto, salvo el destinatario y sus datos adjuntos. Empleamos la función de cartas modelo para generarlas. Es decir, las macros son pequeños programas que permiten al usuario automatizar ciertas tareas que normalmente se ejecutan a mano. Ejemplo: Microsoft Word. Algo característico de ese tipo de virus es que operan en diferentes plataformas (PC, Mac, Unix, etc.) donde funcione el programa. Lo cual les permite ampliar su rango de acción y sus daños asociados. Ejemplo los virus que existieron en los programas de Microsoft Office

1995-2000. Este periodo se caracteriza por los virus conocidos como “virus de Internet/Correo Electrónico”. El advenimiento y desarrollo de los sistemas de comunicación por mensajes electrónicos, trajo consigo, aparte de comunicación instantánea, el desarrollo de virus que se distribuían precisamente por mensajería electrónica. Y atrajeron la atención de los usuarios con títulos sugestivos que motivaban la curiosidad de los usuarios. Tal es el caso de virus como Melissa y el famoso virus I LOVE YOU. Cuyo título era tan sugestivo, que pocas personas evitaron abrir un mensaje de correo con este título, y sobre todo si venía de personas conocidas del usuario.

2000-a la fecha. A partir del año 2000 comienza el desarrollo y los ataques furtivos, de grandes porporciones que realizan los virus conocidos como Virus Mezclados. Los virus mezclados son aquellos que combinan características de aquellos virus que en el pasado tuvieron un impacto considerable sobre los sistemas informáticos. Lo cual le da la facultad al virus de evadir programas antivirus. Ejemplo de estos virus: Worm_Klez.H, Worm_Bagle, Worm_MyDoom.A, Worm_Netsky.

Ante este panorama la pregunta que nos hacemos es:

¿Cómo detectar un virus?

Los síntomas que denotan que una computadora está infectada por un virus son:

Mensajes extraños en la pantalla de la computadora.

Pérdida aparentemente inexplicable de información en la computadora.

Lentitud extrema del equipo o un funcionamiento errático que provoca que se bloquee, se apague sola y vuelva a encender.

La computadora se conecta a internet sin haber hecho clic en la conexión destinada para ello.

Si la computadora está en una red de alguna empresa o compañía, se nota una lentitud muy notoria para enviar y recibir correos electrónicos, para imprimir.

Nuestros conocidos, de quienes tenemos sus direcciones de correo electrónico reciben mensajes de parte nuestra, cuando nosotros ni siquiera hemos enviado mensajes a ellos.

Y pasamos al siguiente pregunta:

¿Cómo eliminar un virus?

Si bien el escenario informático sigue amenazado por la existencia de nuevos virus, cada vez más agresivos. Se pueden tomar ciertas medidas para minimizar el impacto de tales amenazas, entre las que se puede mencionar:

1. La mejor manera de proteger la información de una computadora es contar con un software antivirus.
2. Mantener actualizada su protección antivirus. La cual debe estar siempre actualizada, esto es; con las últimas vacunas contra los virus más nuevos.
3. Actualización de "parches" de seguridad para equipos con Microsoft Windows. Los parches de seguridad son arreglos que se hacen a un programa del cual se tiene noticia de que posee una vulnerabilidad que puede o es aprovechada por la gente que crea virus. Estos parches son indispensables para un funcionamiento adecuado de un antivirus y del sistema mismo.
4. No abrir mensajes de correo de personas que no conocemos o bien cuyos títulos en los mensajes no son de confianza por ser en otros idiomas, las direcciones de correo tienen nombre sumamente raros.
5. Evitar navegar en páginas de Internet inseguras: de sexo principalmente.

¿Qué hacer cuando un virus ha atacado un sistema o a una red?

El ataque de un virus hacia una red o hacia las computadoras, implica que alguna de acciones preventivas mencionadas anteriormente no se cumplió. Y si el equipo cuenta con un antivirus, lo más probable es que el mismo esté desactualizado en cuanto a listas de virus se refiere o bien esté dañado, ya que existen virus que lo primero que atacan es a los programas antivirus.

Los pasos que hay que seguir ante una situación de infección por virus es:

1. Verificar si su sistema de protección antivirus esta funcionando correctamente
2. Existen páginas en internet de las diferentes marcas de antivirus que tienen herramientas de limpieza contra los virus a las cuales se podrá acceder. Y se puede hacer la búsqueda de los virus desde la página del fabricante antivirus.

Sin embargo, ¿Cual sería la protección ideal si ahora?...

¿Cuento con un antivirus actualizado y sigo teniendo equipos infectados o atacados dentro de la red y no logro identificar la fuente de tales ataques?

El modelo tradicional de las soluciones o productos de antivirus, con foco en la optimización de los tiempos de desarrollo de vacunas, resulta ineficaz e inadecuado en el escenario actual, ya que no pueden asegurar en tiempo y forma el desarrollo de las vacunas necesarias que permitan proteger a las empresas y evitar el despliegue de los virus dentro de las estructuras informáticas de las mismas.

Es por esto que se debe buscar una solución que nos de lo siguiente:

1. Dormir tranquilo y asegurarme de que los programas antivirus trabajen en forma automática al detectar y eliminar los virus en la red.
2. Que la solución prevenga y proteja antes de que el virus intente atacar la red.
3. Que si bien los sistemas operativos de Microsoft sufren de vulnerabilidades, y son un medio de ataque de los virus, entonces que algo me ayude a realmente cubrir o aislar tales vulnerabilidades y evitar además el ingreso de virus que pretendan aprovechar esas vulnerabilidades.
4. Un antivirus instalado en la red que automáticamente siempre este actualizado sin necesidad incluso de que lo haga una persona manualmente.
5. Estar seguro que el 100% de los equipos con que cuento en la empresa tienen su antivirus actualizado y que no falta ninguno de proteger, y tener la certeza de que todos los equipos instalados en la empresa están actualizados en cuanto a parches de seguridad se refiere... sean 10, 50, 500 o 1000 equipos.
6. Que los recursos del área de Tecnología de Información se destinen a proyectos de desarrollo y crecimiento de la corporación y no a hacer limpiezas manuales de virus.

ESTIMADO SOCIO

Cualquier comentario, observación o sugerencia a este Boletín, favor de hacerlo llegar directamente al autor.

Ing. Arturo Fernández Maldonado
mailto:arturo.fernandez@trendtyc.com