Virus: Su Historia y su Desarrollo

Salvador Lara Rocha[1], Mario Rojas[1], Leonel Rodríguez[1], Jose G. Hernández[1] & M. Farias-Elinos[2]

[1]Laboratorio de Interoperabilidad de la UANL
{slara,mrojas,lrogdriguez}@dsi.uanl.mx, josherna@mail.uanl.mx
[2] Lab. de Investigación y Desarrollo de Tecnología Avanzada (LIDETEA)
Escuela de Ingeniería / Coordinación General de Investigación,
ULSA, Benjamín Franklin 47,
Col. Hipódromo Condesa ,
México, D.F., 06140, México
elinos@ci.ulsa.mx

Introducción

La aparición de los primeros virus informáticos se remonta a 1986

En este año, Basit y Amjad se percataron de que el sector de arranque de una unidad de disco contenía código ejecutable, y que este código corría siempre que se reiniciaba la computadora con un disco en A: . También se dieron cuenta de que podía reemplazar código con su propio programa, pudiendo ser éste un programa en la memoria residente, y que podía instalar una copia de sí mismo en cada disco, accesible desde cualquier dispositivo. Como el programa se copiaba a sí mismo, le dieron el nombre de 'virus', por su semejanza con los virus biológicos. Este proyecto de virus solamente infectó 360Kb de discos.

También en 1986, un programador llamado Ralf Burger vio que un archivo podía hacer una copia de sí mismo por el método simple de adjuntarse en otros archivos. Entonces desarrolló una demostración de este efecto, que llamó 'Virdem'. Lo distribuyó en la 'Chaos Computer Conference' de diciembre de ese año, en la cual el tema principal eran precisamente los virus. La demostración tuvo tanto éxito que Burger escribió un libro sobre el tema, en el que no se mencionaba aún a los virus del sector de arranque.

Al siguiente año, Franz Swoboda tuvo noticia de un virus incluido en un programa llamado 'Charlie'. Por ello, le llamó el 'Virus Charlie'. Hubo mucho revuelo en la opinión pública acerca de este virus, al difundirse las dos versiones de una misma historia: Burger afirmó que había obtenido una copia del virus de manos de Swoboda, pero Swoboda lo negó siempre. En cualquier caso, Burger se hizo con esa copia que envió a Bernt Fix, el cual 'desarmó' el virus, y Burger incluyó en su libro la demostración del análisis, después de añadirle varios parches para variar su comportamiento. El comportamiento normal de 'Vienna' (o 'Charlie', como lo llamaba Swoboda) era colocar un archivo entre otros ocho para reiniciar la computadora (el virus 'parchea' los primeros cinco bytes de código); Burger (o quizá Fix) reemplazaron este código con cinco espacios. El efecto fue que los archivos 'parcheados' inhibían a la computadora, en vez de reiniciarla. No era una mejora muy satisfactoria.

Mientras tanto, en los Estados Unidos Fred Cohen acababa de completar su tesis doctoral, que versaba precisamente sobre los virus informáticos. El doctor Cohen demostró que uno no puede escribir un programa que sea capaz de, con un cien por cien de aciertos, visualizar un archivo y decidir si es o no un virus. Desde luego, nadie pensó jamás en esa posibilidad, pero Cohen hizo buen uso de un teorema matemático, y así fue como se ganó el doctorado. Sus experimentos sobre la difusión de virus en los sistemas informáticos

demostraron que la expansión de las infecciones resultaba ser mucho más rápida de lo que nadie hubiera esperado.

Cohen visitó la Universidad Lehigh, y allí se encontró con Ken van Wyk. De este encuentro surgió el virus 'Lehigh', que nunca abandonó el laboratorio, porque sólo podía infectar COMMAND.COM y dañar increíblemente su huésped después de tan sólo cuatro replicaciones. Una de las reglas básicas sobre los virus es que aquel de ellos que dañe de forma muy rápida su huésped, no sobrevive durante mucho tiempo. De todas formas, el virus Lehigh se hizo muy popular, y fomentó la aparición del grupo de noticias sobre virus de Ken van Wyk en Usenet.

1988 Este año será recordado siempre entre los expertos en seguridad informática como "el año en el que empezó el baile". De hecho, fue el año en el que comenzaron a aparecer los fabricantes de anti-virus, creando una moda de lo que en principio sólo era un problema potencial. Los vendedores de software anti-virus eran pequeñas compañías, que ofrecían sus productos a muy bajo precio, en algunos casos gratuitamente.
Fue en este año cuando la compañía IBM se dio cuenta de que tenía que tomarse el asunto de los virus completamente en serio. Esta conclusión no la tomaron debido a la incidencia del popular 'gusano del árbol de Navidad', de amplia difusión, sino porque IBM sufrió un brote del virus 'Cascade', y se encontró en la embarazosa necesidad de tener que comunicar a sus clientes que ellos también habían sido infectados. Desde este momento, el 'High Integrity Laboratory' de IBM fue el encargado del área virus.

En 1988 aparecieron, desde luego, múltiples rebotes de 'Brain', 'Italian', 'Stoned', 'Cascade' y 'Jerusalem'. Esto representó la prueba definitiva de la existencia real de los virus. Peter Norton, en una entrevista, había comentado que eran una leyenda urbana, como los cocodrilos de las alcantarillas de Nueva York, y un experto informático del Reino Unido llegó a proclamar que tenía la prueba de que los virus eran un producto de la imaginación de mentes sin que hacer...

¿Qué es un virus informático?

Un virus informatico es simplemente un programa. Una secuencia de instrucciones y rutinas creadas con el único objetivo de alterar el correcto funcionamiento del sistema y, en la inmensa mayoría de los casos, corromper o destruir parte o la totalidad de los datos almacenados en el disco.

Existen varios tipos de virus de acuerdo a la forma en que se ejecutan:

- Programas: archivos ejecutables con las extensiones: .com, .exe, .drv, .ovl, .sys, .bin, .bat, etc; También archivos con la posibilidad de ejecutar macros, como los .doc, .xls, .ppt, etc.
- Arranque: rutinas que se ejecutan durante el arranque.
- Multipartita: capaces de hacer las dos cosas anteriores.

Así como también se da una clasificación de acuerdo a su funcionamiento:

Virus puro

Un verdadero virus tiene como características más importantes la capacidad de copiarse a sí mismo en soportes diferentes a los que se encontraba originalmente, y por supuesto hacerlo con el mayor sigilo posible y de forma transparente al usuario; a este proceso de autorréplica se le conoce como "infección", de ahí que en todo este tema se utilice la terminología propia de la medicina: "vacuna", "tiempo de incubación", etc. Como soporte entendemos el lugar donde el virus se oculta, ya sea fichero, sector de arranque, partición, etc.

Un virus puro también debe modificar el código original del programa o soporte objeto de la infección, para poder activarse durante la ejecución de dicho código; al mismo tiempo, una vez activado, el virus suele quedar residente en memoria para poder infectar así de forma trasparente al usuario.

Caballo de Troya

Al contrario que el virus puro, un Caballo de Troya es un programa maligno que se oculta en otro programa legítimo, y que produce sus efectos perniciosos al ejecutarse este ultimo. En este caso, no es capaz de infectar otros archivos o soportes, y sólo se ejecuta una vez, aunque es suficiente, en la mayoría de las ocasiones, para causar su efecto destructivo.

Bomba Lógica

Se trata simplemente de un programa maligno que permanece oculto en memoria y que solo se activa cuando se produce una acción concreta, predeterminada por su creador: cuando se llega a una fecha en concreto (Viernes 13), cuando se ejecuta cierto programa o cierta combinación de teclas, etc.

Gusano o Worm

Por último, un gusano en un programa cuya única finalidad es la de ir consumiendo la memoria del sistema, mediante la realización de copias sucesivas de sí mismo, hasta desbordar la RAM, siendo ésta su única acción maligna.

La barrera entre virus puros y el resto de programas malignos es muy difusa, prácticamente invisible, puesto que ya casi todos los virus incorporan características propias de uno o de varios de estos programas: por ejemplo, los virus como el Viernes 13 son capaces de infectar otros archivos, siendo así virus puro, pero también realizan su efecto destructivo cuando se da una condición concreta, la fecha Viernes 13, característica propia de una bomba lógica; por último, se oculta en programas ejecutables teniendo así una cualidad de Caballo de Troya. De ahí la gran confusión existente a este respecto.

¿Cómo funciona un virus?

Los virus sólo se activan cuando el programa infectado es ejecutado o cuando el registro de arranque es leído. En el momento que se activan, ejecutan su rutina, y pueden realizar cualquier acción no deseada sin que el usuario lo note.

Los virus residentes en los registros de arranque, pueden infectar archivos o ejecutarse, cuando leemos una unidad de disco o cualquier otro dispositivo. Los otros virus sólo pueden realizar acciones cuando el archivo infectado es ejecutado. Los archivos que sólo contienen datos, no pueden ser infectados, dado que no pueden ejecutar ninguna rutina, pero sí pueden ser dañados.

Antes de nada, hay que recordar que un virus no puede ejecutarse por si solo, necesita un programa portador para poder cargarse en memoria e infectar; asimismo, para poder unirse a un programa portador necesita modificar la estructura de este, para que durante su ejecución pueda realizar una llamada al código del virus

Las partes del sistema más susceptibles de ser infectadas son el sector de arranque de las unidades de disco, la tabla de partición y el sector de arranque del disco duro, y los ficheros ejecutables (*.EXE y *.COM). Para cada una de estas partes tenemos un tipo de virus, aunque muchos son capaces de infectar por sí solos estos tres componentes del sistema.

En las unidades de disco, el sector de arranque es una zona situada al principio del disco, que contiene datos relativos a la estructura del mismo y un pequeño programa, que se ejecuta cada vez que arrancamos desde la unidad de disco.

En este caso, al arrancar con un disco contaminado, el virus se queda residente en memoria RAM, y a partir de ahí, infectara el sector de arranque de todos las unidades de disco a las que se accedan, ya sea al formatear o al hacer un DIR en el disco, dependiendo de cómo esté programado el virus.

¿Cómo se realiza el proceso de infección?

El proceso de infección consiste en sustituir el código de arranque original del disco por una versión propia del virus, guardando el original en otra parte del disco; a menudo el virus marca los sectores donde guarda el código de arranque original como en mal estado, protegiéndolos así de posibles accesos, esto suele hacerse por dos motivos: primero, muchos virus no crean una rutina propia de arranque, por lo que una vez residente en memoria, efectúan una llamada al código de arranque original, para iniciar el sistema y así aparentar que se ha iniciado el sistema como siempre, con normalidad. Segundo, este procedimiento puede ser usado como técnica de ocultamiento.

¿Cuáles son los efectos de los virus?

Los efectos perniciosos que causan los virus son variados; entre éstos se encuentra él formateo completo del disco duro, eliminación de la tabla de partición, eliminación de archivos, ralentización del sistema hasta limites exagerados, enlaces de archivos destruidos, archivos de datos y de programas corruptos, mensajes o efectos extraños en la pantalla, emisión de música o sonidos

¿Cuales son las características principales de los virus?

Un virus puede tener más de una de las siguientes características:

Residir en Memoria: Un programa puede cargarse en la memoria del ordenador, y desde allí infectar todos los archivos ejecutables que se usen, y monitorear cualquier acción que el usuario realice.

No Residir en Memoria: No se cargan en memoria, por lo tanto sólo pueden correr rutinas infecciosas cuando el programa infectado es ejecutado.

Ocultamiento (Stealth): Un virus puede esconderse de los antivirus, en forma completa, redirigiendo la lectura del disco hacia otro sector, o modificando la información para que el antivirus no detecté que el archivo fue modificado.

Encriptación: este es otro método de ocultación, por el cual el virus permanece encriptado hasta que se ejecuta..

Polimorfismo: un virus polimórfico tiene la capacidad de mutar, cambiando parte de su programación para lucir distinto de un momento a otro.

Ejecutables por evento (Trigger o Payload): capaces de ejecutarse cuando un evento sucede en la PC. Por ejemplo, ejecutarse en una fecha en especial, o cuando el usuario apaga la computadora, etc.

Multipartito: aquellos virus que son capaces de infectar tanto archivos como sectores de arranque.

¿Cuales son los síntomas más comunes cuando tenemos un virus?

Reducción del espacio libre en la memoria o disco duro.
Un virus, cuando entra en un ordenador, debe situarse obligatoriamente en la memoria RAM, y por ello ocupa una porción de ella. Por tanto, el tamaño útil operativo de la memoria se reduce en la misma cuantía que tiene el código del virus.

Frecuentes caídas del sistema operativo.

Las operaciones rutinarias se realizan con mas lentitud.

Aparición de programas residentes en memoria desconocidos.

Tiempos de carga mayores.

Aparición de mensajes de error no comunes.

Fallos en la ejecución de los programas.

Actividad y comportamientos inusuales de la pantalla.
Muchos de los virus eligen el sistema de vídeo para notificar al usuario su presencia en el ordenador. Cualquier desajuste de la pantalla, o de los caracteres de esta nos puede notificar la presencia de un virus.

El disco duro aparece con sectores en mal estado
Algunos virus usan sectores del disco para camuflarse, lo que hace que aparezcan como dañados o inoperativos.

Cambios en las características de los ficheros ejecutables
Casi todos los virus de fichero, aumentan el tamaño de un fichero ejecutable cuando lo infectan. También puede pasar, si el virus no ha sido programado por un experto, que cambien la fecha del fichero a la fecha de infección.

Aparición de anomalías en el teclado
Existen algunos virus que definen ciertas teclas que al ser pulsadas, realizan acciones perniciosas en el ordenador. También suele ser común el cambio de la configuración de las teclas, por la del país donde se programo el virus.

¿ Qué es un programa antivirus?

Para combatir la avalancha de virus informáticos se creó el software antivirus. Estos programas suelen incorporar mecanismos para prevenir, detectar y eliminar virus. Para la prevención se suelen usar programas residentes que alertan al usuario en todo momento de cualquier acceso no autorizado o sospechoso a memoria o a disco, por lo que resultan sumamente útiles al impedir la entrada del virus y hacerlo en el momento en que este intenta la infección, facilitándonos enormemente la localización del programa maligno. Sin embargo presentan ciertas desventajas, ya que al ser residentes consumen memoria RAM, y pueden también resultar incompatibles con algunas aplicaciones. Por otro lado, pueden llegar a resultar bastante molestos, puesto que por lo general suelen interrumpir nuestro trabajo habitual con el ordenador avisándonos de intentos de acceso a memoria o a disco que en muchos casos provienen de programas legítimos. A pesar de todo, son una medida de protección excelente y a ningún usuario debería faltarle un programa de este tipo.

Existen varios métodos que utilizan los antivirus para detectar virus informáticos:

- Búsqueda por Cadena de Caracteres: Una cadena de caracteres es una parte de código o información que contiene datos únicos que pertenecen a la codificación de un virus. Los antivirus buscan dentro de los archivos estas cadenas de caracteres que tienen almacenadas en sus bases de datos. Este método es el más común entre muchos programas antivirus.

- Búsqueda por Algoritmo: Este método inspecciona ciertas características que aparecen normalmente en archivos infectados y sí existen, determina que el archivo examinado está infectado. Para esto, los antivirus utilizan una base de datos que contiene las relaciones entre los virus y sus formas de actuar.

- Método de Vacunación: En este caso los antivirus guardan información acerca de los archivos del disco donde se encuentran instalados, y los chequean para saber si sufrieron cambios o no, lo que algunas veces se debe a actividad vírica.

- Método de Investigación: Consiste de la prueba de las capacidades de un supuesto virus encontrado en memoria para conocer si el mismo tiene capacidades de infección.

- Método de Anti-Ocultamiento: Sólo puede ser utilizado cuando el virus ya se encuentra activo. Previene que aplicaciones o virus manipulen los recursos del sistema para modificar el código original del sistema o aplicación.

- Detección heurística: esta es una de las fórmulas más avanzadas de remotorización de virus. La búsqueda de virus mediante esta técnica se basa en el desensamblado del código del programa que se intenta analizar con el objetivo de encontrar instrucciones (o un conjunto de ella) sospechosas.

- Los programa antivirus buscan remover las rutinas maliciosas dentro de los archivos infectados de lo contrario sugieren al usuario borrar dichos archivos.

¿Qué es un agujero de seguridad?

Un agujero de seguridad o una vulnerabilidad, es un error en una aplicación o sistema operativo por el cual se compromete la confiabilidad de la información y del equipo donde se está ejecutando dicho programa vulnerable.

Cualquier persona malintencionada que tenga acceso a esta aplicación o sistema puede aprovechar los agujeros de seguridad y causar graves daños a la información contenida en el equipo, dependiendo del alcance de la vulnerabilidad.

Consejos para evitar la infección de un Virus

Dada la gran propagación de virus informáticos, no basta con tener un antivirus instalado para estar protegido de ellos. Por ello, aquí listamos algunos consejos útiles que ayudarán a los usuarios de computadoras para estar prevenidos de estos maliciosos programas.

Tener activada la Protección antivirus en Macros de las aplicaciones del Office Word, Excel, PowerPoint.

Mantener constantemente actualizado el antivirus que tengan instalado, para que sea capaz de detectar los últimos virus.

No abrir ni ejecutar archivos ejecutables que no hayan sido solicitados por usted y sean recibidos por correo electrónico, aunque sea desde una fuente confiable. Si es necesario ejecutarlo, antes sanéelo con un antivirus confiable y actualizado.

Es indispensable tener un disquete de arranque libre de virus para poder iniciar la computadora con él en caso de infección.

Si utiliza disquetes, protéjalos contra escritura antes de utilizarlo en otras computadoras.

Realice un resguardo o backup periódico de aquella información que usted considere indispensable, y no desee perderla.

Cambie la configuración de la secuencia de arranque, para que el equipo siempre intente iniciar el sistema en principio desde el disco C. De esta manera se evitará la acción de cualquier virus de arranque puro que pueda usted tener en alguna unidad de disco. Cuando deba iniciar desde la unidad de disco, tan sólo deberá cambiar nuevamente la configuración de la secuencia de arranque.

Suscríbase a un servicio de alertas de virus para estar al tanto de los últimos virus detectados.

En el caso de servidores es necesario un manejo especial en cuanto a medidas para no infectarse; se debe de instalar un antivirus el cual filtre la información entrante, así como también aplicar políticas sobre el tipo de archivos restringidos.

No reenvíe cualquier alerta de virus que reciba por e-mail que no venga de una fuente calificada, dado que muchas de ellas son falsas alarmas.

Las medidas de prevención pasan por el control, en todo momento, del software ya introducido o que se va a introducir en nuestro ordenador, comprobando la fiabilidad de su fuente. Esto implica la actitud de no aceptar software no original, ya que él pirateo es una de las principales fuentes de contagio de un virus, siendo también una practica ilegal y que hace mucho daño a la industria del software .

Por supuesto, el sistema operativo, que a fin de cuentas es el elemento software más importante del ordenador, debe ser totalmente fiable; si éste se encuentra infectado, cualquier programa que ejecutemos resultara también contaminado. Por eso, es imprescindible contar con una copia en disquetes del sistema operativo, protegidos éstos

contra escritura; esto ultimo es muy importante, no solo con el sistema operativo sino con el resto de disquetes que poseamos. Es muy aconsejable mantenerlos siempre protegidos, ya que un virus no puede escribir en un disco protegido de esta forma.

El riesgo de contraer un virus en la Internet es menor que de cualquier otra manera, tanto los mensajes de correo, como la página WEB transfieren datos. Sólo si se trae un software por la red y lo instala en su máquina puede contraer un virus.